Technologies émergentes pour la transformation numérique

Dominique Luzeaux

Ingénieur général de l'armement, HDR. Ambassadeur de la transformation numérique et conseiller spécial auprès du Commandant suprême allié transformation (*SACT*).

À l'échelle mondiale, les organisations sont soumises à une mutation profonde, induite par l'accélération technologique et la multiplication des crises environnementales. L'interconnexion croissante des systèmes rend la maîtrise des dynamiques mondiales indispensable à la pérennité de toute organisation. Face à cette complexité, l'adaptation est impérative, car tout faux pas risque de compromettre durablement la compétitivité. La transformation numérique, en intégrant les technologies numériques à tous les niveaux de l'entreprise, révolutionne les modèles opérationnels et la création de valeur pour le client. Les outils numériques facilitent la communication, le partage des connaissances et la collaboration entre des équipes diverses, quelle que soit leur situation géographique. Les technologies émergentes, quant à elles, accélèrent cette mutation, bouleversant les industries et ouvrant de nouveaux horizons.

Ce changement de paradigme est tout aussi pertinent, voire plus encore, dans le domaine militaire. Comme le montre le conflit ukrainien, la victoire ne dépend pas uniquement de la quantité de matériels, mais aussi des systèmes et services numériques innovants qui l'enrichissent, ainsi que de l'ingéniosité de ceux qui les utilisent. Pour maintenir notre supériorité, il est nécessaire d'évoluer d'une approche centrée sur les plateformes vers une stratégie globale, renforcée par le numérique, qui donne la priorité aux effets militaires souhaités. L'interaction dynamique des capacités émergentes, l'interconnexion accrue des systèmes et l'explosion des données exigent une approche de la défense et de la dissuasion résolument numérique. Les données et les technologies ne sont plus de simples outils, mais des éléments fondamentaux de notre posture stratégique. Cette mutation profonde permet aux forces armées d'accroître leur efficacité, de générer des effets innovants et de gagner en agilité, en flexibilité et en évolutivité.

Cette mutation nécessite de passer d'architectures traditionnelles et statiques vers des systèmes dynamiques, centrés sur les données et intégrant des technologies de pointe. Il est cependant primordial de prendre en compte les implications éthiques et sociétales de ces avancées afin de garantir un développement durable et

équitable. Les enjeux liés à la protection des données personnelles et aux biais inhérents aux algorithmes nécessitent une approche responsable de l'utilisation de ces technologies.

Le monde numérique repose sur plusieurs éléments clés qui fonctionnent ensemble pour créer l'environnement interconnecté d'aujourd'hui :

- matériaux et équipements physiques ;
- logiciels et paradigmes algorithmiques ;
- réseaux : l'infrastructure permettant l'interconnexion et le transfert de données ;
- données : ceci inclut leur stockage, et les traitements employés pour gérer et exploiter efficacement les technologies numériques, en particulier les mesures de cybersécurité.

Ces éléments constituent collectivement l'épine dorsale du monde numérique. Des avancées technologiques se produisent à tous les niveaux de ces composants, ainsi que dans leurs nouvelles combinaisons aux niveaux des sous-systèmes et des systèmes.

Microélectronique et paradigmes informatiques

Le monde moderne repose sur le transistor, un composant à l'échelle nanométrique intégré à des milliards d'exemplaires sur des circuits imprimés. La prise en compte du numérique commence au niveau des matières premières et progresse à travers l'assemblage en couches de minuscules commutateurs, pour aboutir à des systèmes informatiques à grande échelle. Pour dépasser les limites de la loi de Moore, nous devons explorer des techniques de fabrication innovantes et de nouveaux paradigmes informatiques capables de tirer parti des innovations à tous les niveaux de la pile technologique.

Au-delà du flux d'électrons traditionnel, les nouveaux matériaux comme la spintronique et la ferroélectricité offrent de nouvelles approches informatiques. La spintronique exploite les propriétés des champs magnétiques et du spin des électrons, tandis que la photonique exploite la puissance de la lumière pour la transmission de données. Les circuits intégrés photoniques, qui intègrent des composants optiques sur des micropuces, représentent une avancée significative dans le domaine de l'informatique. Ces circuits offrent des avantages considérables par rapport à leurs homologues électroniques, notamment des vitesses de transmission de données plus élevées, une perte de signal réduite sur de longues distances et une miniaturisation accrue. Cela est particulièrement avantageux pour les applications dans les centres de données, le calcul haute performance et les télécommunications : les signaux optiques peuvent parcourir de plus longues distances sans perte significative de puissance du signal, réduisant ainsi le besoin d'amplification du signal gourmande en énergie.

Les dispositifs spintroniques, tels que les transistors à effet de champ de spin (Spin-FET), utilisent le spin des électrons pour contrôler le flux de courant, ce qui pourrait conduire à des solutions plus rapides et plus économes en énergie. Les matériaux ferroélectriques présentent une polarisation électrique spontanée qui peut être inversée en appliquant un champ électrique externe. Cette propriété leur permet de maintenir la polarisation sans alimentation externe, ce qui les rend adaptés aux dispositifs de mémoire non volatile et aux condensateurs. De plus, leurs capacités de changement de forme en réponse aux champs électriques les rendent précieux pour les actionneurs et les capteurs.

La consommation d'énergie reste un défi majeur en informatique. L'augmentation de la vitesse d'horloge entraîne une augmentation de la dissipation de chaleur. L'informatique neuromorphique, qui utilise des dispositifs à très faible consommation d'énergie comme les memristors et les semi-conducteurs magnétiques dilués, offre une piste potentielle. Les dispositifs supraconducteurs, tels que les jonctions Josephson, permettent des circuits rapides et économes en énergie en éliminant la résistance électrique. Cependant, ces dispositifs nécessitent un refroidissement cryogénique pour exploiter pleinement leur potentiel.

Le calcul réversible, basé sur des circuits réversibles, offre une autre voie d'amélioration de l'efficacité énergétique. En minimisant la dissipation d'énergie pendant le calcul, ces systèmes offrent des avantages théoriques. Les portes photoniques quantiques Fredkin-Toffoly illustrent ce principe, même si la vitesse reste un défi de taille. Le développement de nouveaux algorithmes et d'une pile logicielle entièrement nouvelle est essentiel pour exploiter pleinement le potentiel de ces paradigmes émergents.

Informatique ADN

L'informatique ADN est une approche informatique non conventionnelle qui exploite les propriétés uniques des molécules d'ADN, de la biochimie et du matériel de biologie moléculaire pour effectuer des calculs.

Le calcul ADN utilise des réactions biochimiques et des techniques de biologie moléculaire pour manipuler et traiter les brins d'ADN. Ces opérations peuvent être conçues pour effectuer des opérations logiques, telles que les portes *AND*, *OR* et *NOT*. L'un des principaux avantages du calcul ADN est sa capacité à effectuer des calculs parallèles massifs. Des milliards de molécules d'ADN peuvent être traitées simultanément, ce qui peut conduire à des accélérations significatives pour certains types de problèmes. Cela a été utilisé pour résoudre des problèmes d'optimisation complexes, tels que celui du voyageur de commerce, où l'objectif est de trouver le chemin le plus court à travers un ensemble de villes. Cependant, les molécules d'ADN sont sujettes à des erreurs lors de la réplication et de la manipulation, et le développement de techniques de correction d'erreurs robustes est

essentiel pour un calcul fiable ADN. De plus, la lecture des résultats des calculs ADN peut prendre du temps et être sujette à des erreurs.

Les molécules d'ADN sont également incroyablement efficaces pour stocker des informations, car chaque brin d'ADN contient une séquence de nucléotides qui peuvent représenter des données binaires. Elles ont le potentiel de stocker de vastes quantités de données sous une forme compacte (plusieurs pétaoctets dans un gramme) et durable (des milliers d'années si elles sont stockées correctement, sans nécessiter d'énergie pour conserver les données stockées).

Bien que l'informatique ADN en soit encore à ses débuts, elle promet de révolutionner l'informatique en offrant des niveaux de parallélisme et de capacité de stockage sans précédent.

Surfaces intelligentes reconfigurables

La demande mondiale en matière de connectivité sans fil à haut débit, à faible latence et à faible consommation d'énergie ne cesse de croître. Les surfaces intelligentes reconfigurables exploitent des métamatériaux, des algorithmes sophistiqués et des techniques avancées de traitement du signal pour transformer des surfaces ordinaires en composants intelligents pour la communication sans fil. Ces surfaces bidimensionnelles, composées de matériaux techniques, possèdent des propriétés reconfigurables qui permettent un contrôle dynamique de la propagation des ondes électromagnétiques réfléchies. En manipulant leurs caractéristiques électriques et magnétiques de la surface, elles peuvent être programmées pour optimiser la communication sans fil, la localisation, la détection et le transfert d'énergie sans fil.

Leur nature hautement adaptative permet des ajustements en temps réel aux conditions environnementales changeantes et aux demandes des utilisateurs, optimisant ainsi l'utilisation des ressources.

Packaging *avancé et spécialisation des puces*

Le *packaging* avancé et la spécialisation des puces sont deux tendances dans l'industrie des semi-conducteurs, motivées par la recherche incessante de performances supérieures, d'une consommation d'énergie plus faible et de facteurs de forme plus petits pour des appareils électroniques de plus en plus complexes.

Le *packaging* avancé englobe un ensemble de techniques permettant l'intégration de plusieurs puces dans un seul boîtier. Cette intégration, réalisable dans des configurations 2D et 3D, conduit à une densité plus élevée, à des performances améliorées et à une consommation d'énergie réduite.

La spécialisation des puces implique la décomposition de conceptions complexes de systèmes sur puce en puces plus petites et spécialisées. Cette approche rationalise les processus de conception, de fabrication et de test, tout en permettant l'optimisation des performances et de la consommation d'énergie grâce à l'utilisation de diverses technologies de processus pour différents composants du système.

Capteurs et informatique quantiques

Les capteurs quantiques offrent une précision et une sensibilité sans précédent, ouvrant des perspectives nouvelles pour le champ de bataille du futur. Avec des capacités de détection et de surveillance avancées dans divers domaines et conditions, quel que soit le jour ou la nuit, la météo ou la disponibilité des systèmes mondiaux de navigation par satellite (GNSS), les capteurs quantiques peuvent révolutionner les opérations militaires. Les interféromètres quantiques (accéléromètres et gravimètres), les magnétomètres, les horloges atomiques et les radars quantiques sont des exemples clés de ces technologies. Ces dispositifs quantiques surpassent considérablement leurs homologues classiques, offrant une précision considérablement accrue dans la cartographie des signaux magnétiques, électriques et gravitationnels.

Les accéléromètres et gyroscopes basés sur l'Interférométrie à atomes froids (*CAI*) permettent une navigation autonome sur le long terme et un positionnement précis des systèmes maritimes et spatiaux. Les gravimètres quantiques, qui mesurent les niveaux gravitationnels absolus, trouvent des applications dans les levés géophysiques, l'exploration du terrain et la détection d'objets et d'installations souterrains. Les magnétomètres quantiques, en particulier les dispositifs d'interférence quantique supraconducteurs (*SQUID*), offrent une sensibilité exceptionnelle et sont essentiels aux capacités modernes de renseignement, de surveillance et de reconnaissance, y compris la détection des sous-marins nucléaires. Le radar quantique, avec sa capacité à détecter des objets à faible réflectivité et à fonctionner avec une faible probabilité d'interception, représente une avancée significative en matière de télédétection.

L'informatique quantique est un domaine révolutionnaire qui s'appuie sur les principes de la mécanique quantique pour résoudre des problèmes complexes, insolubles pour les ordinateurs classiques. Ce changement de paradigme repose sur trois concepts fondamentaux : les qubits, la superposition et l'intrication. Les qubits, l'équivalent quantique des bits classiques, peuvent exister dans plusieurs états simultanément, ce qui permet un traitement parallèle massif et des calculs exponentiellement plus rapides. La superposition permet aux qubits d'explorer plusieurs solutions simultanément, tandis que l'intrication permet l'interconnexion des qubits, quelle que soit la distance, facilitant ainsi les calculs complexes et le traitement réparti de l'information.

Les tendances actuelles en informatique quantique se concentrent sur des approches modulaires, où plusieurs processeurs quantiques de taille plus petite sont interconnectés pour améliorer l'évolutivité et les performances. Alors que le nombre de qubits dans les processeurs quantiques continue de croître, des progrès significatifs sont réalisés dans les techniques de correction d'erreurs quantiques pour garantir la précision et la fiabilité des calculs quantiques. Le développement d'algorithmes quantiques efficaces qui peuvent surpasser les algorithmes classiques s'accélère, élargissant les applications potentielles de l'informatique quantique. En outre, des efforts sont en cours pour intégrer les systèmes informatiques quantiques et classiques, créant des approches hybrides qui exploitent les atouts des deux technologies.

Réseaux 5G

Dans le monde des télécommunications, les réseaux mobiles de cinquième génération (*5G*) représentent des vitesses plus élevées, une latence plus faible et une plus grande capacité pour les réseaux de données. La *5G* permet également des communications massives de machine à machine, et la possibilité de mettre en œuvre des réseaux virtuels grâce au découpage du réseau (« *network slicing* »).

Les nouvelles technologies comme *Open RAN* (*Open Radio Access Network*) s'inscrivent dans un mouvement plus large vers des architectures de réseau plus ouvertes et plus flexibles, ce qui est particulièrement important à l'heure où la *5G* et les technologies futures continuent d'évoluer. *Open RAN* est une approche de construction de réseaux mobiles qui favorise l'interopérabilité et la normalisation des éléments du réseau d'accès radio. Elle permet aux équipements de différents fournisseurs de fonctionner ensemble de manière transparente grâce à des interfaces et des protocoles standardisés. Elle prend en charge l'utilisation de technologies définies par logiciel et de virtualisation, ce qui facilite la mise à l'échelle et l'adaptation du réseau à l'évolution des demandes, d'où une flexibilité et une évolutivité accrues. Et avec une chaîne d'approvisionnement plus diversifiée et des protocoles de sécurité standardisés, elle peut améliorer la sécurité globale des réseaux mobiles.

Cependant, les systèmes *5G* ont encore une capacité limitée. La technologie de sixième génération (*6G*) des réseaux mobiles établira de nouvelles normes pour répondre aux exigences de performance inaccessibles de la *5G*. Cela est dû aux exigences élevées en matière de réseau plus intelligent, de latence ultra-faible, de vitesse de communication réseau extrême et de prise en charge d'un grand nombre d'applications connectées diverses. Les avantages de la *6G* iront au-delà de la vitesse de transmission des données, offrant un meilleur accès à *Internet*, des taux de transmission élevés, un faible délai et une large bande passante. La *6G* s'appuie sur la technologie *5G*. Elle étend la numérisation grâce à des capacités uniques telles que les antennes à entrées multiples et sorties multiples sans cellule (*MIMO*),

une technologie adaptée à la communication tactique sans fil. De telles antennes à chaque extrémité du circuit de communication sont combinées pour minimiser les erreurs, optimiser la vitesse des données et améliorer la capacité des transmissions radio en permettant aux données de circuler sur plusieurs chemins de signaux en même temps. En outre, la *6G* repose sur des surfaces intelligentes et des capacités supérieures grâce aux fréquences térahertz.

La cybersécurité est un autre domaine crucial que la *6G* devra aborder. La lutte contre les cybermenaces nécessite un mélange d'héritage et d'innovation. Les technologies émergentes comme le cryptage quantique sont essentielles pour résoudre des problèmes qui dépassent la portée des stratégies actuelles. La *6G* devrait garantir des communications sécurisées, même dans le contexte des progrès de l'informatique quantique.

Cloud Computing

Le *Cloud Computing* offre une évolutivité inégalée, permettant aux entreprises d'ajuster de manière dynamique leurs ressources informatiques et technologiques en réponse aux fluctuations de la demande. En accélérant le déploiement de nouvelles applications et de nouveaux services, le *Cloud Computing* favorise l'innovation et améliore les délais de mise sur le marché. En outre, il offre un accès transparent aux données, améliorant ainsi l'agilité organisationnelle dans l'environnement commercial actuel en constante évolution. Les fournisseurs de *cloud* investissent massivement dans des infrastructures redondantes et des mesures de reprise après des sinistres robustes, garantissant des niveaux élevés de fiabilité et de disponibilité. Des protocoles de sécurité rigoureux, tels que le chiffrement, les contrôles d'accès et les audits réguliers, protègent les données sensibles et aident les entreprises à se conformer aux exigences réglementaires.

Si le *Cloud Computing* offre des avantages considérables, le *Edge Computing* offre une solution décentralisée qui rapproche la puissance de traitement des sources de données. En déployant des applications et des services à la périphérie du réseau, les entreprises peuvent réduire la latence, améliorer les performances et renforcer la confidentialité des données. Le *Edge Computing* réduit considérablement la latence en traitant les données localement, améliorant ainsi les performances des applications et l'expérience utilisateur, en particulier pour les applications à faible latence, à bande passante élevée ou hors ligne. Il renforce également la confidentialité des données en minimisant leur transfert et en les traitant au plus près de leur source, réduisant ainsi le risque de leur violation et garantissant la conformité aux réglementations locales. Le *Edge Computing* améliore la fiabilité du système en offrant une redondance et une tolérance aux pannes, atténuant ainsi l'impact des pannes du centre de données central. Enfin, il optimise le trafic réseau et réduit les coûts de bande passante en traitant les données localement.

Le changement de paradigme du *Cloud Computing* vers l'*Edge Computing* peut être étendu au *Far Edge Computing*, qui rapproche encore plus la puissance de traitement des sources de données, souvent au sein de capteurs ou d'actionneurs. Il offre une latence ultra-faible et des capacités de traitement hautement localisées, ce qui le rend idéal pour les applications qui nécessitent un traitement de données immédiat et efficace, telles que les systèmes de contrôle en temps réel et les infrastructures critiques. Bien que les nœuds *Far Edge* aient une puissance de traitement limitée, ils sont optimisés pour des tâches ou des fonctions spécifiques, garantissant un traitement des données efficace et efficient.

Blockchains *et infrastructures physiques décentralisées*

Une *blockchain* est un registre numérique décentralisé et distribué qui enregistre les transactions sur plusieurs ordinateurs, garantissant ainsi la sécurité et l'intégrité des données. Chaque transaction est encapsulée dans un bloc, et ces blocs sont liés entre eux de manière cryptographique, ce qui rend pratiquement impossible la modification des données historiques. En tant que paradigme informatique, les *blockchains* exploitent la décentralisation et les algorithmes cryptographiques pour assurer la transparence, la sécurité, la traçabilité et l'immuabilité. Elles facilitent la vérification d'identité sécurisée et fiable, permettent la mise en réseau *peer-to-peer* et les processus automatisés qui favorisent la confiance et la responsabilité, réduisant ainsi la dépendance à l'égard de tiers centralisés.

Des efforts sont en cours pour améliorer l'interopérabilité de la *blockchain*, autorisant des transferts de données et d'actifs fluides sur différents réseaux. L'évolutivité et la vitesse des transactions sont traitées grâce à des innovations telles que le *sharding* et les solutions *layer-2*, qui permettent le traitement hors chaîne et le regroupement des transactions.

L'infrastructure physique décentralisée (*DePin*) est une approche révolutionnaire en matière de conception, de construction et d'exploitation des systèmes et infrastructures physiques de manière décentralisée. En tant que réseau basé sur la *blockchain*, *DePin* permet aux nœuds de fournir des données de manière décentralisée. En exploitant les principes de la *blockchain*, *DePin* favorise la transparence, l'efficacité et l'accessibilité dans la gestion des infrastructures, réduisant ainsi la dépendance aux systèmes centralisés traditionnels. Cela permet d'envisager un avenir où les systèmes physiques sont interconnectés, autonomes et autogérés, conduisant à des opérations plus efficaces, résilientes et durables.

Filecoin est un réseau de stockage décentralisé qui utilise la technologie *blockchain* pour inciter les utilisateurs à stocker et à récupérer des données. En tirant parti des incitations économiques (la quantité de stockage disponible et le prix des données stockées sont contrôlés par le marché libre basé sur la *blockchain* et sa monnaie associée), *Filecoin* garantit un stockage de données fiable et précis.

Les utilisateurs peuvent sélectionner des mineurs de stockage (participants au réseau qui utilisent la puissance de calcul pour valider et enregistrer les transactions sur la *blockchain*) en fonction de facteurs tels que le coût, la redondance et la vitesse, en les payant en monnaie *blockchain* pour stocker leurs données. Les nœuds de récupération, chargés de localiser et de récupérer les données, sont incités à fournir un service rapide et efficace. L'une des caractéristiques uniques de ce réseau est son architecture différenciée, séparant les nœuds de stockage et de récupération. Cela incite un large éventail de participants, y compris les utilisateurs de taille moyenne, à contribuer à la décentralisation du réseau. Les nœuds de récupération, stratégiquement situés à proximité des nœuds de stockage, sont optimisés pour une bande passante élevée et une faible latence, garantissant une récupération efficace des données.

Construire des réseaux sécurisés et résilients de nouvelle génération avec une conscience numérique

S'appuyant sur les technologies et paradigmes précédents, la détection et les communications intégrées sont des technologies émergentes qui combinent les capacités de communication et de détection sans fil dans un seul système. En utilisant les mêmes signaux de radiofréquence à des fins de communication et de détection, elle optimise l'utilisation des ressources et rassemble les capacités de détection et de communication dans un seul système. En exploitant le grand nombre d'antennes des appareils sans fil modernes, elle peut fournir des capacités de détection haute résolution, notamment la détection d'objets, la localisation et la cartographie de l'environnement.

Cela permet aux réseaux sans fil de prendre en compte l'environnement et d'améliorer les architectures de l'*Internet* des objets (*IoT*). La technologie optique sans fil intègre des capacités de détection et de communication : les systèmes d'éclairage et d'affichage peuvent s'intégrer de manière transparente à l'écosystème sans fil. Les surfaces éclairées peuvent servir de nœuds de réseau, facilitant la communication et la détection sans interférence électromagnétique. *Via* cette technologie, il est possible de surveiller l'infrastructure, de collecter et d'analyser des données pour obtenir des informations précieuses et d'automatiser les processus. Cependant, pour exploiter pleinement son potentiel, il faut établir des normes de communication et assurer une coordination au niveau du réseau.

La recherche de systèmes de réseaux et de communications interopérables, filaires et sans fil de nouvelle génération est cruciale, car elle permet un accès partout et à tout moment, même lorsque les infrastructures physiques (terrestres) ne sont pas disponibles. De nombreuses données, produits et services sont fournis par quelques satellites en orbite, des actifs nationaux et commerciaux offrant de grandes capacités, mais dont l'architecture ne garantit pas un niveau élevé de résilience. En raison de la mécanique orbitale, chaque type d'orbite présente des

avantages et des inconvénients, en termes de couverture, de résolution, de temps de revisite et de capacité à transmettre rapidement des données aux utilisateurs sur Terre. Bien que les récentes méga-constellations comptant jusqu'à des milliers de satellites aient déclenché un changement de paradigme dans la manière de fournir des services tout en garantissant la résilience, ces actifs sont exposés à divers types de menaces (naturelles et intentionnelles), ce qui entraîne un risque de lacunes majeures dans la fourniture de services.

Plateformes à haute altitude

Il est possible de combler le fossé entre *Internet* et la stratosphère grâce à des stations à haute altitude, généralement sous forme de ballons, qui améliorent la connectivité là où les infrastructures de communication traditionnelles ne sont pas disponibles. De telles plateformes offrent une connectivité, une couverture et des performances améliorées que ni les satellites ni les tours terrestres ne peuvent égaler.

En fait, le défi consiste à tirer parti de toutes les technologies et de tous les moyens possibles pour collecter et diffuser des données et des informations. En d'autres termes, comment gérer de la manière la plus holistique et la plus agile possible les quatre couches inférieures du modèle *OSI* (*Open Systems Interconnection*) à 7 couches (physique, liaison de données, réseau, transport). Cela nécessite un équilibre évolutif entre le matériel et le logiciel, d'autant plus que le développement des réseaux et de l'intelligence artificielle sera de plus en plus étroitement lié à mesure que l'IA jouera un rôle croissant dans la gestion et l'animation de réseaux dotés de plus de puissance de détection et de calcul.

Réseaux définis par logiciel

Le réseau défini par logiciel (*SDN*) a révolutionné la gestion des réseaux en découplant le plan de contrôle du plan de données. Ce changement architectural repose sur la séparation du plan de contrôle (responsable de la gestion et du contrôle de la manière dont les paquets de données sont transmis sur le réseau) du plan de données (responsable du mouvement réel des paquets de données sur le réseau), centralisant l'intelligence du réseau dans un contrôleur programmable. Cela permet une gestion, une optimisation et une automatisation plus efficaces des ressources réseau. Le *SDN* offre des avantages significatifs, notamment une agilité, une évolutivité et une sécurité améliorées pour les réseaux à grande échelle.

Sa nature programmable, facilitée par des *API* (*Application Programming Interfaces*) ouvertes, permet des changements de configuration rapides et des ajustements dynamiques et automatisés du comportement du réseau, tels que le provisionnement, le dépannage et l'application des politiques. Cela permet aux organisations de s'adapter rapidement à l'évolution des demandes du réseau et de faire évoluer les ressources en fonction des besoins. Le *SDN* fait abstraction de

l'infrastructure réseau sous-jacente, ce qui permet la création de réseaux virtuels pouvant être gérés de manière indépendante. Le contrôle centralisé, la micro-segmentation, le contrôle d'accès basé sur des politiques et la détection automatisée des menaces améliorent la sécurité du réseau. De plus, les analyses avancées du réseau, alimentées par l'apprentissage automatique, permettent aux organisations de surveiller les performances du réseau, d'identifier les goulots d'étranglement et d'optimiser le flux de trafic, réduisant ainsi la latence et améliorant l'efficacité globale du réseau.

La convergence des réseaux *SDN*, *5G*, *Far Edge Computing* et des protocoles de communication *peer-to-peer* émergents offre des opportunités pour des solutions de réseau *peer-to-peer* innovantes dans les environnements mobiles. Cette approche offre une résilience dans des environnements de communication en évolution rapide et potentiellement hostiles. Cependant, assurer une sécurité robuste reste un défi crucial qui nécessite l'intégration de technologies supplémentaires.

Communication quantique, distribution de clés

La communication quantique est un domaine de pointe qui s'appuie sur les principes de la mécanique quantique pour transmettre des informations de manière sécurisée. Elle repose sur deux aspects principaux :

- Bits quantiques (Qubits) : Contrairement aux bits classiques, qui prennent les valeurs soit 0 soit 1, les qubits peuvent exister dans plusieurs états simultanément grâce à la superposition. Cela permet un codage des données plus complexe et plus sécurisé.
- Intrication quantique : ce phénomène relie les qubits de telle manière que l'état d'un qubit influence instantanément l'état d'un autre, quelle que soit la distance qui les sépare.

L'intrication quantique est utilisée pour garantir des canaux de communication sécurisés, par exemple *via* la distribution de clés quantiques (*QKD*). Elle permet à deux parties de produire une clé secrète aléatoire partagée connue d'elles seules. Cette clé peut ensuite être utilisée pour chiffrer et déchiffrer des messages. Étant donné que la *QKD* s'appuie sur des superpositions quantiques ou l'intrication quantique pour transmettre des informations dans des états quantiques, elle garantit que toute tentative d'écoute clandestine de la clé sera détectée, car la mesure d'un système quantique le perturbe et introduit des anomalies détectables.

Malgré son potentiel, la communication quantique est confrontée à des défis tels que le besoin de matériel spécialisé, le maintien de la cohérence des qubits sur de longues distances et l'intégration à l'infrastructure de communication existante. De plus, bien que la *QKD* offre un niveau de sécurité élevé, elle nécessite souvent un canal de communication classique authentifié et du matériel spécialisé, ce qui peut être coûteux et complexe à mettre en œuvre.

Technologies améliorant la confidentialité

La cybersécurité se concentre sur la conformité (respect des réglementations et normes du secteur), la détection et la réponse aux menaces (identification et atténuation des cyberattaques) et la protection des données (protection des informations sensibles contre les cybermenaces). Cette dernière peut être réalisée au moyen de divers schémas de cryptage, au niveau matériel ou logiciel. Le calcul confidentiel se concentre sur l'intégrité et la confidentialité de l'environnement d'exécution, en protégeant les données dans des enclaves sécurisées pendant le traitement : les données sont décryptées dans l'environnement d'exécution de confiance, traitées, puis recryptées si nécessaire. Cependant, cela signifie que les données sont décryptées à un moment donné, ce qui ouvre la voie à des attaques par canal auxiliaire : le véritable défi consiste à traiter informatiquement des données cryptées sans avoir à les décrypter. C'est là que les paradigmes de calcul avancés peuvent être intéressants, permettant l'exploitation des données sans pouvoir accéder aux données réelles.

Chiffrement homomorphe

Le chiffrement homomorphe est une technique cryptographique qui permet d'effectuer des calculs sur des données chiffrées sans les déchiffrer au préalable. Il permet de traiter et d'analyser des données sensibles sans compromettre leur confidentialité. Il facilite le partage et le traitement sécurisés des données dans le *cloud*, permettant aux organisations de tirer parti des services basés sur le *cloud* sans sacrifier la confidentialité des données. Il peut appliquer des algorithmes d'apprentissage automatique et d'IA aux données chiffrées, ouvrant ainsi de nouvelles possibilités d'analyse et de compréhension des données. Enfin, il permet de se conformer aux réglementations sur la confidentialité des données en garantissant que les données restent chiffrées tout au long de leur cycle de vie.

Cependant, les opérations homomorphes nécessitent beaucoup de calculs et tous les types de calcul ne sont pas pris en charge. De plus, la génération, le stockage et la gestion sécurisés des clés sont essentiels à la sécurité des systèmes homomorphes, et leur fuite compromet l'ensemble du système.

Calcul distribué sécurisé

Le calcul distribué sécurisé est une technique cryptographique qui permet à plusieurs parties de calculer en collaboration sur des données partagées sans révéler leurs entrées individuelles. Alors que la cryptographie consiste à dissimuler le contenu, ce type de calcul et de protocole consiste à dissimuler des informations partielles sur les données tout en calculant avec les données provenant de nombreuses sources et en produisant correctement les sorties. Dans un tel calcul, un nombre défini de parties disposent chacune de données privées et calculent la

valeur d'une fonction publique sur ces données privées tout en gardant secrètes leurs propres entrées. Chaque partie divise son entrée en plusieurs parts. Celles-ci sont distribuées aux autres de manière qu'aucune partie ne puisse reconstituer l'entrée d'origine. Les parties effectuent des calculs intermédiaires sur leurs parts ; ces calculs sont conçus pour préserver la confidentialité des entrées. La sortie finale est reconstruite en combinant les parts de toutes les parties. Le protocole garantit que la sortie est correcte et qu'aucune partie n'apprend plus que les informations nécessaires.

Cependant, les protocoles de calcul distribué sécurisés impliquent souvent plusieurs cycles de communication entre les parties, ce qui augmente la latence et la surcharge de communication. Les problèmes de synchronisation et les limitations de bande passante s'ajoutent à ces défis techniques.

De nouvelles frontières dans l'intégration des technologies et des connaissances

De nombreuses nouvelles technologies sont disponibles, améliorant les performances actuelles au niveau des composants. Cependant des solutions encore plus innovantes au niveau système naissent d'une convergence intelligente ou d'une intégration de ces technologies.

IA générative

Les avancées récentes dans le domaine de l'apprentissage profond, des modèles fondamentaux (modèles à grande échelle et à usage général formés sur des ensembles de données divers et étendus) et des grands modèles linguistiques (un sous-ensemble de modèles fondamentaux spécifiquement axés sur les tâches liées au langage) ont propulsé le domaine de l'IA générative. Ces modèles, capables de créer de nouveaux contenus, révolutionnent les secteurs en automatisant les tâches, en générant du contenu créatif et en fournissant des informations précieuses. De la rédaction de rapports à la conception de produits complexes, l'IA générative remodèle le mode de fonctionnement des organisations.

Les modèles d'action de grande taille (*LAM*) représentent la prochaine frontière de l'IA générative, s'étendant au-delà de la génération de texte pour englober des tâches complexes orientées vers l'action. En combinant la compréhension du langage, le raisonnement et l'exécution d'actions, les *LAM* peuvent effectuer des tâches de manière autonome et répondre de manière dynamique à leur environnement. Ils exploitent les atouts des réseaux neuronaux et de l'IA symbolique, ce qui leur permet d'apprendre à partir de données du monde réel et de prendre des décisions éclairées.

L'IA peut améliorer considérablement le réalisme et la complexité des simulations : en s'adaptant et réagissant aux stratégies des joueurs, *via* l'apprentissage, on peut créer ainsi des environnements d'entraînement dynamiques et stimulants. Cela permet de former le personnel à faire face à des menaces en constante évolution et d'accélérer les processus de prise de décision. Le traitement massif de données et l'analyse prédictive fournissent des informations en temps réel sur l'espace de bataille, ce qui permet aux commandants de disposer d'informations essentielles. En identifiant les tendances, en améliorant les tactiques et en prédisant le comportement de l'ennemi, ces technologies offrent un avantage stratégique significatif.

Si l'IA générative est un outil puissant, il est essentiel de l'utiliser de manière éthique et responsable. L'un des principaux défis est la nature « boîte noire » des modèles d'IA, qui rend difficile la compréhension et l'atténuation des biais. La technologie *Blockchain* offre une solution potentielle en offrant transparence et traçabilité dans les systèmes d'IA.

Parmi d'autres approches innovantes dans l'utilisation de l'IA, on peut citer le *co-design* piloté par l'IA. En optimisant l'équilibre entre matériel, *middleware* [1] et logiciel, la conception de puces assistée par IA peut libérer le potentiel des technologies émergentes comme l'informatique quantique, neuromorphique et biologique. Les jumeaux numériques de paradigmes de pointe en microélectronique et informatique permettent la conception de l'atome à l'architecture, élargissant l'accès aux outils de fabrication et aux capacités de prototypage. Cela, à son tour, favorise les progrès de la fabrication additive, où les techniques d'impression 3D créent des objets complexes couche par couche, optimisant l'utilisation des matériaux et la précision de la conception.

De la réalité augmentée et de la réalité virtuelle au métavers

La réalité virtuelle (RV) et la réalité augmentée (RA) sont des technologies immersives qui offrent des expériences distinctes. La RV crée un environnement numérique totalement immersif qui remplace le monde réel, tandis que la RA superpose des informations numériques au monde réel, améliorant ainsi la perception de l'utilisateur. Elles ont toutes deux le potentiel de révolutionner la formation, l'éducation et le divertissement. Associées à la modélisation et à la simulation (M&S), ces technologies permettent de visualiser des prototypes et d'améliorer les processus de conception. En brouillant les frontières entre le monde virtuel et le monde réel, elles offrent une plateforme sûre et efficace pour l'acquisition et le développement des compétences. L'avènement de la *5G* a encore accéléré l'adoption d'expériences immersives en fournissant la bande passante et la vitesse nécessaires.

[1] Logiciel qui fait office de pont entre différents logiciels ou systèmes informatiques. Il se situe entre le système d'exploitation et les applications, et simplifie tous les échanges entre applications.

La convergence de multiples technologies, dont l'IA (par exemple pour la personnalisation *via* des avatars et pour l'analyse des interactions ou des données), la *blockchain*, la neurotechnologie, l'infographie et le matériel informatique avancés, les réseaux *5G* et l'*IoT* (pour transférer des informations entre monde réel et monde virtuel *via* des objets connectés), favorise l'émergence du métavers. Cet espace partagé virtuel collectif, combinant une réalité physique virtuellement améliorée et un espace virtuel physiquement persistant, offre des opportunités d'interaction et de collaboration sans précédent. Le métavers a le potentiel de révolutionner les opérations militaires, de la formation et de la simulation à la planification et à l'exécution des missions. Les commandants peuvent exploiter le métavers pour simuler des scénarios complexes, visualiser les données du champ de bataille et planifier des missions dans un environnement virtuel. En outre, le métavers peut permettre le contrôle à distance de systèmes sans pilote, améliorant ainsi la sécurité et l'efficacité dans des environnements dangereux. En immergeant les utilisateurs dans différents contextes culturels, le métavers peut faciliter la compréhension mutuelle du langage et de la culture, favorisant ainsi l'interopérabilité entre les forces militaires.

Conclusion

La convergence des Nanotechnologies, des biotechnologies, des technologies de l'information et des sciences cognitives (NBIC) a le potentiel de révolutionner les capacités humaines et de relever des défis complexes. Les technologies numériques, en particulier dans le domaine des technologies de l'information, jouent un rôle essentiel dans cette convergence. L'intégration des sciences cognitives et des technologies de l'information favorise le développement d'interfaces cerveau-ordinateur qui peuvent améliorer les capacités cognitives humaines. La synergie entre l'impression 3D et la nanofabrication permet la création de structures complexes à l'échelle microscopique, ce qui conduit à des avancées dans les domaines de la science et de l'ingénierie des matériaux. En outre, la convergence de ces domaines avec la bio-ingénierie ouvre la voie au développement de nouvelles formes « vivantes » capables d'interconnecter des composants à base de silicium avec de la matière organique.

Cependant, l'évolution rapide de ces technologies soulève d'importantes préoccupations éthiques, notamment dans le domaine numérique. Des questions telles que la confidentialité, la sécurité des données et le risque d'utilisation abusive nécessitent un cadre solide pour guider le développement et la mise en œuvre. L'amélioration humaine, à la fois cognitive et physique, et l'impact environnemental des nanomatériaux sont des domaines clés du débat éthique. Le rythme rapide de la convergence technologique dépasse souvent le développement de cadres réglementaires adéquats. Une approche de gouvernance globale est essentielle pour

anticiper et relever les défis éthiques, sociétaux et politiques posés par ces technologies.

Alors que nous continuons d'explorer le potentiel de la convergence NBIC, il est essentiel de trouver un équilibre entre les progrès technologiques et les considérations éthiques, d'équité et d'accès. Pour garantir que ces avancées profitent à la société dans son ensemble, nous devons préserver les droits et libertés individuels et remédier aux inégalités potentielles découlant d'un accès limité. Une approche collaborative impliquant les décideurs politiques, les scientifiques, les éthiciens et le public est nécessaire pour établir des lignes directrices, des normes et des cadres réglementaires qui régissent les technologies émergentes et protègent les consommateurs. ◆

Courriel de l'auteur : dominique.luzeaux@polytechnique.org

Mots-clés : Technologie, quantique, IA, *5G*, *6G*, ADN.