Cybersécurité du soldat augmenté : un nouveau défi pour l'OTAN

Angèle Billaud

Analyste en droit international, sécurité internationale, cybersécurité et défense, diplômée de l'Université Grenoble Alpes, France.

15 octobre 2025

ISSN : 2739-3283

Comment citer cette publication :

Angèle Billaud, *Cybersécurité du soldat augmenté : un nouveau défi pour l'OTAN,* Institut d'études de géopolitique appliquée, Paris, 15 octobre 2025.

Avec le soutien de la division diplomatie publique de l'Otan

Sommaire

Introduction

L'essor des technologies numériques transforme le champ militaire, entre perspective du soldat augmenté et risques cyber préoccupants. À l'échelle de l'OTAN, le développement de ces technologies est également reconnu comme une priorité stratégique permettant de maintenir l'avantage militaire de l'Alliance, tant sur le plan de la dissuasion que de la défense. Cette priorité est notamment retranscrite dans le Concept Otanien *Warfighting Capstone,* adopté en 2021, qui sert « d'étoile polaire » pour le développement d'initiatives stratégiques[1]. Le Concept insiste notamment sur la nécessité de maîtriser plusieurs domaines, en particulier la capacité à assurer l'opérabilité simultanée des forces dans les environnements physiques et virtuels[2].

Les objectifs otaniens se déclinent notamment à travers le développement du soldat augmenté. Ce dernier peut être défini comme :

> « *un soldat dont les capacités sont augmentées, stimulées ou créées dans le but de renforcer son efficacité opérationnelle. Ces augmentations peuvent aller de la modification physiologique, ou d'un changement d'état psychologique, à l'utilisation de moyens qui, faisant corps avec lui, assurent la continuité de l'amélioration de ses capacités corporelles sensorielles, physiques ou cognitives*. »[3]

Dans le cadre du développement des technologies numériques, l'analyse du concept de soldat augmenté portera sur les équipements faisant corps avec le soldat, destinés à accroître ses performances sans nécessiter d'action de sa part. Ainsi, des lentilles de contact intelligentes et connectées peuvent être considérées comme une forme de soldat augmenté, contrairement à un robot, qui requiert une manipulation active[4].

Les objectifs otaniens se traduisent également par le renforcement des capacités de cybersécurité et de cyberdéfense. Il est affirmé, dans la politique de l'OTAN en matière de cyberdéfense et dans son plan d'action adoptés en 2014, que la cyberdéfense constitue une composante de la défense collective au cœur de l'Alliance[5]. Cette politique prévoit une coopération étroite avec l'industrie en vue de développer des technologies et des pratiques essentielles pour remplir cette mission défensive[6]. En ce sens, une cyberdéfense efficace repose nécessairement sur un haut niveau de cybersécurité et de cyberrésilience des infrastructures numériques des forces armées.

---

[1] *NATO Warfighting Capstone Concept*, NATO Allied Command Transformation, 2021, p. 2.
[2] *Id*. p. 17.
[3] DE BOISBOISSEL Gérard, LE MASSON Jean-Michel, *Le soldat augmenté : définitions, Les Cahiers de la Revue de Défense Nationale*, p. 22.
[4] *Id*. p. 21.
[5] *La cyberdéfense à l'OTAN*, Fiche d'information, OTAN, décembre 2016.
[6] *Ibid*.

Si ces deux thématiques font l'objet d'initiatives souvent distinctes, elles restent étroitement liées. L'intégration d'outils numériques au soldat entraîne nécessairement de nouveaux risques cyber. Il apparaît donc essentiel d'examiner comment la cybersécurité conditionne l'efficacité et la viabilité du concept de soldat augmenté dans le cadre otanien.

Le soldat augmenté entre innovation et dépendance technologique

En 1968, Ivan Sutherland, chercheur à Harvard, met au point le dispositif « épée de Damoclès », aujourd'hui reconnu comme le premier casque de réalité augmentée[7]. Au fil des années, cet outil rudimentaire est enrichi de détecteurs de mouvement oculaire, permettant d'adapter les images à chaque nouvelle position du regard, ainsi que de gyroscopes et de technologies de géolocalisation[8]. Aujourd'hui, plusieurs États membres de l'OTAN ont développé leurs propres dispositifs de réalité augmentée destinés à une application militaire. Le Royaume-Uni, par exemple, a conçu un outil fixé au casque du soldat, capable de projeter les images recueillies par le drone Watchkeeper[9]. L'armée de terre française prévoit, quant à elle, d'acquérir un casque de réalité augmentée (RAFT) intégrant un système d'affichage et permettant l'interconnexion des membres d'une unité via Wi-Fi ou Bluetooth[10].

Les augmentations du soldat dépassent également le cadre de la réalité augmentée, en incluant des dispositifs plus intrusifs. Selon une étude publiée en 2017 par le Secrétariat général de la défense et de la sécurité nationale (SGDSN), le développement d'implants visant à améliorer la vision ou l'audition, ainsi que de dispositifs d'électrostimulation cérébrale, pourrait être opérationnel d'ici 2030[11]. Ces technologies, intrusives ou non, reflètent une promesse opérationnelle d'augmenter l'efficacité, la résilience physique et cognitive, et la capacité de traitement d'un plus grand nombre de données, permettant une supériorité décisionnelle. Cette augmentation des capacités des forces est effectivement non négligeable, permettant d'agir plus rapidement et dans la durée.

Toutefois, le développement de ces technologies d'augmentation soulève la question de la dépendance de l'opérabilité des forces à leur fonctionnement. À mesure que ces outils prennent une place croissante dans les stratégies militaires, l'avantage stratégique et l'efficacité opérationnelle qu'ils apportent risquent de créer une dépendance envers ces technologies. Cela entraînerait un risque considérable d'échec des missions en cas de dysfonctionnement des équipements ou des infrastructures de soutien. Si le soldat est entraîné avec ces équipements et

[7] NOEL Jean-Christophe, *A la recherche du soldat augmenté : espoirs et illusions d'un concept prometteur,* IFRI, Laboratoire de recherche sur la défense, septembre 2020, p. 21.
[8] *Ibid*.
[9] *Id*. p. 22.
[10] *Ibid*.
[11] DE BOISBOISSEL Gérard, LE MASSON Jean-Michel, *Le soldat augmenté : définitions, op.cit*. p. 25.

dépend de leurs performances, il se retrouverait dans un flou opérationnel dangereux pour sa mission et pour lui-même en cas de panne ou de dysfonctionnement.

Cette perspective souligne deux priorités stratégiques dans le développement d'outils d'augmentation. D'une part, il convient d'entraîner le soldat à poursuivre une opération sans ces équipements, notamment à travers des exercices ciblés et un apprentissage sur les capacités et limites de ces technologies. Un des objectifs majeurs devrait notamment être d'éviter une sur-confiance dans ces technologies, afin que le soldat les traite comme un soutien opérationnel plutôt qu'un remplaçant de sa propre analyse du champ de bataille. D'autre part, il convient de limiter le plus possible les dysfonctionnements de ces équipements pour bénéficier de leurs promesses opérationnelles. Cela se traduit notamment par la mise en place d'une cybersécurité robuste des équipements, des pratiques et des infrastructures de soutien.

L'intégration de la cybersécurité comme condition de supériorité opérationnelle

Au-delà des incidents techniques, le fonctionnement des technologies d'augmentation est menacé par les interférences ennemies. Cela inclut notamment les intrusions et sabotages contre les équipements du soldat, permettant de falsifier son positionnement ou son accès aux communications ; les attaques de manipulation de l'information, à travers l'injection de fausses données dans des systèmes d'intelligence artificielle destinés au ciblage par exemple ; ou encore les attaques sur les infrastructure de soutien, comprenant les clouds et les réseaux satellitaires permettant de stocker les données stratégiques et d'assurer les communications entre unités. Ces attaques représentent un risque considérable pour les forces, pouvant mener à des fratricides par falsification du ciblage, à l'augmentation du brouillard du champ de bataille par l'injection de fausses informations, et à un désavantage opérationnel majeur à travers l'accès aux communications stratégiques.

Par ailleurs, ces attaques peuvent être menées par un spectre d'acteurs extrêmement large, ce qui accroît considérablement le risque. En effet, la plupart des technologies intégrées au soldat augmenté, notamment l'intelligence artificielle, sont des technologies dites à double usage, c'est-à-dire également accessibles au secteur civil[12]. Leur maîtrise ne permet pas seulement d'en exploiter les bénéfices, mais aussi d'identifier et de cibler leurs vulnérabilités. Parallèlement, l'apprentissage des techniques de cybersécurité est aujourd'hui largement accessible, ce qui facilite l'entrée dans des pratiques de piratage. Ainsi, les menaces ne proviennent pas uniquement de grandes puissances dotées de capacités technologiques avancées, mais également d'acteurs civils, y compris criminels ou terroristes. Face à l'ampleur

[12] *Tendances scientifiques et technologiques 2025-2045*, OTAN Science & Technology Organisation (STO), volume 1, 9 avril 2025, p. 18.

de ces menaces, l'absence d'une sécurité robuste rendrait les technologies intégrées plus vulnérables qu'avantageuses.

Dans le cadre d'une opération menée par l'OTAN, ce risque prend une dimension supplémentaire. La logique de défense collective propre à l'Alliance repose en effet sur l'interopérabilité des forces, ce qui suppose que les équipements puissent se connecter à travers différents réseaux nationaux. Dans ce contexte, une attaque visant un seul équipement ou une seule infrastructure pourrait compromettre l'ensemble des systèmes à l'échelle de l'OTAN, et par conséquent menacer le succès de l'opération. Cette perspective souligne l'importance cruciale d'assurer la cybersécurité des technologies développées par les États membres, non pas par des initiatives isolées, mais dans le cadre d'un effort collectif et coordonné.

La cybersécurité du soldat augmenté face aux défis stratégiques de l'OTAN

En matière cyber, plusieurs obstacles se dressent entre l'OTAN et le développement efficace d'un soldat augmenté. Le principal réside dans la fragmentation persistante entre les États alliés, tant sur leurs priorités stratégiques que sur leurs régulations et leur accès aux ressources technologiques[13]. En fonction de ces facteurs, les Alliés arbitrent différemment entre le développement de quelques équipements très performants mais coûteux, ou un déploiement plus large de systèmes moins sophistiqués[14]. Dans le domaine du soldat augmenté, cette logique se traduit par une multiplication de programmes nationaux fragmentés, rendant difficile l'établissement d'une norme commune en matière de cybersécurité. Cette hétérogénéité génère des vulnérabilités partagées et compromet la capacité de l'Alliance à garantir une interopérabilité complète, condition pourtant essentielle à l'exercice d'une défense collective efficace.

L'OTAN a pris conscience de cette difficulté et cherche à y remédier à travers une série d'initiatives dédiées aux technologies émergentes et de rupture (TE/TR). Le Concept stratégique de 2022 insistait déjà sur la nécessité d'investir dans l'innovation au service des trois missions principales de l'Alliance : dissuasion et défense, prévention et gestion de crise, et sécurité coopérative[15]. De même, le *Capstone Concept* a souligné l'importance de tirer parti des TE/TR pour obtenir un avantage militaire durable, tant pour soutenir l'effort de guerre que pour se prémunir de leur utilisation hostile[16]. Plus récemment, l'OTAN a lancé l'Accélérateur d'innovation de défense pour l'Atlantique Nord (DIANA) ainsi qu'un fonds d'innovation doté

[13] *Tendances scientifiques et technologiques 2025-2045*, STO, *op.cit*. p. 40.
[14] *NATO Science and Technology Strategy*, NATO Science & Technology Organisation (STO), 5 juin 2025, p. 5.
[15] *Id*. p. 4.
[16] *Ibid*.

d'un milliard d'euros, visant à renforcer la coopération avec les industries privées et à accélérer l'adoption de technologies de rupture[17].

Toutefois, la dimension cyber reste encore marginalement intégrée dans ces stratégies. Or, sécuriser le soldat augmenté ne se limite pas à l'acquisition de nouvelles technologies mais exige également une convergence normative et industrielle en matière de cybersécurité entre l'OTAN, l'Union européenne et les États membres. La majorité des Alliés étant membre de l'Union européenne, l'articulation entre les deux systèmes est cruciale. L'Union européenne a déjà développé ses propres instruments en matière de cybersécurité, tels que le règlement sur la cyberrésilience et le règlement sur la cybersécurité, en cours de révision[18]. Elle finance également des projets capacitaires via la Coopération structurée permanente (PESCO) et le Fonds européen de défense. Tandis que la *Boussole stratégique* (2022) insiste sur la nécessité de renforcer la cyberdéfense et la coopération avec l'OTAN, un manque d'ajustement entre les initiatives européennes et otaniennes risque de créer des duplications, voire des contradictions, qui ralentiraient l'intégration technologique. L'alignement de standards OTAN avec les normes européennes constituerait un premier pas vers une véritable interopérabilité normative, évitant aux forces armées d'avoir à composer avec des cadres concurrents.

À ces défis institutionnels s'ajoute la complexité des stratégies nationales. Les États-Unis ont par exemple fait du programme *soldier lethality* une priorité visant à accroître les capacités offensives du combattant[19], tandis que des pays comme la France[20] ou l'Allemagne[21] insistent davantage sur la protection du soldat, l'interopérabilité des systèmes et l'intégration de l'intelligence artificielle. Cette mosaïque d'équipements et de priorités, reflet de cultures stratégiques et de contraintes budgétaires différentes, complique la mise en place d'un socle cyber commun. L'OTAN, en tant que cadre multilatéral, reste la seule enceinte capable de transformer cette diversité en avantage militaire collectif, en imposant des standards minimaux partagés et en garantissant que chaque soldat augmenté, quel que soit son pays d'origine, puisse opérer de manière sécurisée et interopérable.

Concrètement, l'OTAN pourrait établir un socle minimal d'exigences communes en matière de cybersécurité, idéalement aligné avec les normes européennes afin d'éviter les duplications et contradictions. Au regard des contraintes liées au soldat augmenté, ce socle devrait reposer sur l'intégration de mécanismes de sécurité *by design* afin d'incorporer, dès la conception des équipements, des solutions de protection adaptées et de réduire les vulnérabilités susceptibles d'apparaître tout au long de la chaîne de fabrication et d'approvisionnement. D'autres

[17] *Technologies émergentes et technologies de rupture*, site de l'OTAN, consulté le 15 septembre 2025.
[18] Il convient de préciser que les règlements cités excluent de leur champ d'application les produits et activités relevant exclusivement du domaine de la défense ou de la sécurité nationale. Toutefois, compte tenu de l'intégration croissante du secteur public dans les activités liées à la défense, notamment à travers l'utilisation de produits et de services numériques civils soumis à ces régulations, il demeure nécessaire de prendre en considération les impacts indirects de ces textes sur le secteur de la défense.
[19] FREEDBERG Sydney, *Soldier lethality: from G.I Joe to Iron Man,* Breaking Defense, eBRIEF, 2019, p. 1-8.
[20] DE BOISBOISSEL Gérard, LE MASSON Jean-Michel, *Le soldat augmenté : définitions.*
[21] *Germany and Rheinmetall Agree on Gigantic Contract for Future Soldier System,* Army Recognition, Defense News Army, 7 février 2025.

exigences pourraient concerner l'évaluation de la résilience des équipements et les conditions de leur utilisation, afin d'assurer une protection continue face à l'évolution des menaces.

Dans cette logique, la mise en place de standards et d'une certification « OTAN » obligatoires pour l'ensemble des États parties constituerait une étape décisive. Ces standards favoriseraient la sécurité et la résilience des équipements, tout en renforçant leur interopérabilité à travers un plus grand nombre d'États. Ils contribueraient également à consolider la confiance des utilisateurs, élément indispensable à l'efficacité opérationnelle des technologies déployées.

Enfin, l'OTAN pourrait compléter ce dispositif par une évaluation continue des équipements, fondée sur des tests de résilience réguliers, des audits de conformité et des analyses de risques systématiques. Une telle approche garantirait une amélioration constante du niveau de cybersécurité au sein de l'Alliance et des différentes formes du soldat augmenté développées par les Alliés.

Un autre enjeu majeur réside dans la dépendance croissante à l'égard du secteur privé[22]. En effet, la majorité des innovations nécessaires au soldat augmenté, telles que les capteurs biométriques, les systèmes d'IA embarqués et les réseaux de communication sécurisés, sont conçues par des acteurs civils. Leur intégration dans l'écosystème de défense impose d'inventer des mécanismes de confiance, tels que des certifications conjointes OTAN/UE ou des obligations de cybersécurité contractualisées, à l'image du Cybersecurity Maturity Model Certification (CMMC) mis en place par le Département de la Défense américain[23]. Cela permettrait de renforcer la résilience collective tout en évitant une dépendance excessive vis-à-vis d'acteurs extérieurs à l'Alliance. Cet enjeu touche directement à la question de la souveraineté technologique, dans un contexte où les chaînes d'approvisionnement mondialisées constituent autant d'opportunités que de vulnérabilités.

Ainsi, l'OTAN fait face à un paradoxe : elle affiche une volonté affirmée d'intégrer les technologies émergentes et de rupture dans sa stratégie, mais elle peine encore à dépasser la fragmentation interne qui freine la mise en place d'un socle commun, particulièrement en matière de cybersécurité. Tant que cette intégration restera incomplète, l'efficacité opérationnelle du soldat augmenté demeurera compromise, tout autant que la capacité de l'Alliance à répondre de manière unie et cohérente aux défis technologiques et sécuritaires de demain.

[22] *Tendances scientifiques et technologiques 2025-2045*, STO, *op.cit*. p. 39-44.
[23] *Cybersecurity Maturity Model Certification (CMMC),* Department of Defense, décembre 2024.

Conclusion

L'intégration des technologies numériques dans la sphère militaire, notamment à travers le concept de soldat augmenté, ouvre des perspectives inédites en matière d'efficacité opérationnelle et de supériorité stratégique. Pourtant, ces avancées reposent sur une dépendance technologique dont les vulnérabilités peuvent être exploitées, transformant l'innovation en facteur de fragilité. L'expérience récente des conflits, en particulier en Ukraine, rappelle que la domination sur le champ de bataille repose tout autant sur la robustesse des infrastructures numériques que sur la puissance matérielle.

Alors que certaines sources évoquent la possibilité d'une attaque russe contre l'OTAN dans les cinq prochaines années, la dimension cyber du développement des équipements militaire revêt une urgence particulière[24]. En effet, Moscou bénéficie d'une expérience considérable dans l'emploi du cyber comme levier de guerre, au détriment des pays alliés. Dans ce contexte, la cybersécurité apparaît non pas comme un enjeu périphérique, mais comme une condition centrale du succès militaire. Les menaces cyber sont multiples et elles évolueront de manière exponentielle avec la généralisation de l'IA, des implants et des systèmes autonomes. La résilience des forces augmentées, soit leur capacité à opérer même sous attaque, dépendra directement de la qualité de la sécurisation des équipements et des réseaux.

Face à ce défi, l'OTAN fait face à des obstacles de fragmentation qui limitent l'intégration de la cybersécurité des TE/TR et, par extension, du soldat augmenté au cœur de ses stratégies. Les initiatives actuelles sont prometteuses, mais mériteraient d'inclure davantage l'aspect cyber, élément clé de l'efficacité opérationnelle. Une approche intégrée et collective, où la sécurité est pensée « by design » et où l'interopérabilité n'est pas un objectif secondaire, mais une exigence fondamentale, contribuerait à renforcer la résilience collective tout en facilitant l'adoption harmonieuse de ces nouvelles technologies.

À court terme, l'OTAN pourrait établir un socle minimal d'exigences cyber pour le développement d'équipement à composant numérique, aligné avec les normes européennes. À moyen terme, l'Alliance pourrait envisager la création d'un centre d'excellence dédié à la cybersécurité de ces nouveaux équipements, sur le modèle du CCDCOE de Tallinn, et intégrer systématiquement ces enjeux dans ses exercices multinationaux. À long terme, seule une convergence OTAN–UE–États membres permettra de dépasser la fragmentation actuelle et de garantir la résilience du soldat augmenté face aux menaces émergentes.

En définitive, le soldat augmenté ne pourra constituer un avantage opérationnel décisif que si son développement s'accompagne d'une réflexion stratégique approfondie. La cybersécurité doit être considérée comme l'ossature invisible de cette transformation, garantissant à la fois

[24] VAN WAGENEN Matthew, DAVID Arnel, JENSEN Benjamin, *Innovate or Die: The Army Transformation Initiative and the Future of Allied Land Warfare*, Center for Strategic and International Studies (CSIS), 10 juillet 2025.

l'efficacité des forces et la confiance des combattants dans les outils qui les accompagnent. L'Alliance a ici l'occasion de transformer une vulnérabilité potentielle en levier de supériorité, à condition d'agir de manière concertée, anticipative et tournée vers la résilience. Faute d'une cybersécurité robuste et partagée, le soldat augmenté ne serait pas un atout stratégique, mais une vulnérabilité amplifiée.

Bibliographie

Cybersecurity Maturity Model Certification (CMMC), Department of Defense, décembre 2024
https://dodcio.defense.gov/cmmc/About/

DE BOISBOISSEL Gérard, LE MASSON Jean-Michel, *Le soldat augmenté : définitions, Les Cahiers de la Revue de Défense Nationale*, p.21-26
https://www.defnat.com/e-RDN/vue-article-cahier.php?carticle=165&cidcahier=1138

FREEDBERG Sydney, *Soldier lethality: from G.I Joe to Iron Man,* Breaking Defense, eBRIEF, 2019, pp. 8
https://breakingdefense.com/2019/10/new-ebrief-soldier-lethality-from-g-i-joe-to-iron-man/

Germany and Rheinmetall Agree on Gigantic Contract for Future Soldier System, Army Recognition, Defense News Army, 7 février 2025
https://armyrecognition.com/news/army-news/2025/germany-and-rheinmetall-agree-on-gigantic-contract-for-future-soldier-system

La cyberdéfense à l'OTAN, Fiche d'information, OTAN, décembre 2016
https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_12/20161201_1612-factsheet-cyber-defense-fr.pdf

NATO Science and Technology Strategy, NATO Science & Technology Organisation (STO), 5 juin 2025, pp.20
https://www.nato.int/cps/fr/natohq/news_236107.htm

NATO Warfighting Capstone Concept, NATO Allied Command Transformation, 2021, pp.24
https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/

NOEL Jean-Christophe, *A la recherche du soldat augmenté : espoirs et illusions d'un concept prometteur,* IFRI, Laboratoire de recherche sur la défense, septembre 2020, pp.68
https://www.ifri.org/fr/etudes/la-recherche-du-soldat-augmente-espoirs-et-illusions-dun-concept-prometteur

Technologies émergentes et technologies de rupture, site de l'OTAN, consulté le 15 septembre 2025
https://www.nato.int/cps/fr/natohq/topics_184303.htm

Tendances scientifiques et technologiques 2025-2045, OTAN Science & Technology Organisation (STO), volume 1, 9 avril 2025, pp.52
https://www.nato.int/nato_static_fl2014/assets/pdf/2025/4/pdf/250409-STO-Trends-fr.pdf

Une boussole stratégique pour l'Union européenne, Union Européenne, 2022, https://www.consilium.europa.eu/fr/policies/strategic-compass/

VAN WAGENEN Matthew, DAVID Arnel, JENSEN Benjamin, *Innovate or Die: The Army Transformation Initiative and the Future of Allied Land Warfare*, Center for Strategic and International Studies (CSIS), 10 juillet 2025 https://www.csis.org/analysis/innovate-or-die-army-transformation-initiative-and-future-allied-land-warfare

Institut
EGA

ISSN : 2739-3283

Institut d'études de géopolitique appliquée
121 rue du Vieux Pont de Sèvres 92100 Boulogne-Billancourt
Courriel : secretariat@institut-ega.org
Site internet : www.institut-ega.org