LES ARMES AUTONOMES ET LES DÉFIS DE LEUR RÉGULATION

UNE GUERRE SANS SOLDATS... MAIS AVEC QUELLES RÈGLES ?

Dirk NAESSENS

© *Dirk Naessens*

*De opkomst van autonome wapensystemen (***autonomous weapons systems***, AWS) stelt het internationale recht, de militaire doctrines en onze strategische autonomie op de proef. Kunnen we algoritmen vertrouwen om dodelijke beslissingen te nemen? Wie draagt de verantwoordelijkheid als er iets misloopt? Terwijl grootmachten in sneltempo investeren, pleit België voor menselijk toezicht, internationale regulering en technologische soevereiniteit. Maar hoe regelt men iets waarvoor zelfs geen eensgezinde definitie bestaat? Dit artikel neemt u mee in een juridisch en ethisch mijnenveld, dat intussen geen sciencefiction meer is.*

Le lieutenant-colonel d'aviation Dirk NAESSENS, attaché militaire auprès de la représentation permanente de la Belgique à Genève, est membre permanent de l'équipe de négociation belge au sein du groupe d'experts gouvernementaux chargé d'élaborer les éléments d'un cadre juridique et opérationnel pour les systèmes d'armes autonomes.

L'avènement de l'intelligence artificielle (IA) et son intégration croissante dans les capacités militaires soulèvent des questions fondamentales quant à l'avenir de la guerre et à la stabilité internationale. Au cœur de ces discussions se trouvent les systèmes d'armes autonomes (SAA), souvent désignés par l'acronyme anglais AWS (*autonomous weapons systems*). Ces systèmes suscitent des débats intenses au sujet de leur usage militaire et des risques qu'ils posent pour la stabilité internationale. Leur capacité à sélectionner et à engager des cibles sans intervention humaine significative soulève des questions éthiques, juridiques, opérationnelles et sécuritaires majeures. Alors que certaines nations considèrent ces technologies comme un avantage militaire décisif, d'autres alertent sur la nécessité d'une régulation stricte afin d'éviter des conséquences imprévisibles sur les conflits armés.

L'introduction des SAA dans les doctrines militaires bouleverse la conception classique du commandement et du contrôle. Fonctionnant à partir d'algorithmes d'apprentissage automatique, ces systèmes redéfinissent la prise de décision sur le champ de bataille. Cette nouvelle donne soulève une interrogation fondamentale : une machine peut-elle être tenue responsable d'une action militaire ? La responsabilité des SAA pose un défi inédit, car ces systèmes n'ont pas de personnalité juridique propre et ne peuvent donc être tenus directement responsables de leurs actes. En droit international humanitaire, l'État (ou la partie au conflit) porte la responsabilité première.[1] Les commandants[2,3] ainsi que toute personne – y compris les dirigeants de sociétés d'armement[4] – peuvent toutefois engager leur responsabilité pénale individuelle lorsqu'ils participent sciemment à des violations.

[1] Conventions de Genève I à IV, article 1 commun : « Les Hautes Parties contractantes s'engagent à respecter et à faire respecter la présente Convention en toutes circonstances. »

[2] Le Protocole additionnel I aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (1977), article 86, dispose que les supérieurs ne sont pas exonérés de responsabilité lorsque des subordonnés commettent une infraction, s'ils savaient ou auraient dû savoir et n'ont pas agi. Ce protocole n'est toutefois pas universellement ratifié ; parmi les parties non-signataires figurent les États-Unis, Israël, l'Inde et le Pakistan.

[3] Le protocole additionnel I, article 87 impose aux commandants des obligations positives : donner les instructions nécessaires, veiller à ce que les subordonnés connaissent leurs obligations juridiques, et prendre des mesures pour prévenir ou réprimer les violations. Même réserve quant à la portée géographique que pour la note précédente.

[4] L'article 25, § 3 (c), du Statut de Rome de la Cour pénale internationale (1998), explique que toute personne est pénalement responsable si elle facilite, encourage ou contribue de toute autre manière à la commission d'un crime entrant dans la compétence de la Cour. Le Statut de Rome n'est pas universel ; des États majeurs comme les États-Unis, la Russie, la Chine ou Israël n'y sont pas parties.

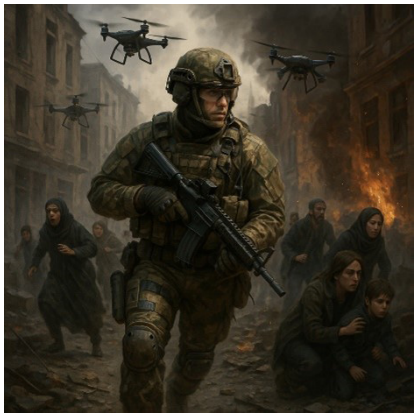


Illustration générée par l'IA

Plusieurs approches sont envisagées pour gérer cette responsabilité. La première consiste à renforcer la responsabilité du commandement militaire, en considérant que toute utilisation d'un SAA relève de la chaîne de commandement existante. Cette approche suit le principe général de la responsabilité du commandement (*command responsibility*), qui impose aux supérieurs hiérarchiques de veiller à ce que les actions de leurs subordonnés soient conformes au droit. C'est par ailleurs l'approche qui est défendue par la Belgique. Toutefois, cela peut devenir complexe lorsque les décisions sont prises par un système autonome sans supervision humaine significative (*meaningful human control).*

Une seconde approche met en avant la responsabilité des concepteurs et des fabricants, en exigeant que les entreprises développant ces technologies intègrent des mécanismes de contrôle garantissant le respect du droit international en général et du droit international humanitaire en particulier. Cette piste pourrait s'inspirer de la réglementation en vigueur dans d'autres industries sensibles, comme l'aviation ou la biomédecine. Cette optique soulève cependant la question de la traçabilité des décisions prises par l'IA et de la possibilité d'anticiper tous les comportements d'un système évolutif.

Certains experts plaident enfin pour la création d'un cadre spécifique de responsabilité internationale, similaire aux régimes existants pour les armes de destruction massive.[5] Ils estiment qu'une telle réglementation permettrait de clarifier les obligations des États et des industriels dans le développement et l'usage des SAA, tout en assurant une meilleure protection du droit international humanitaire. Cela pourrait inclure une interdiction de certaines catégories

[5] Human Rights Watch, *Mind the Gap – The Lack of Accountability for Killer Robots* (Cambridge : International Human Rights Clinic & Harvard Law School, 2015), https://www.hrw.org/sites/default/files/reports/arms0415_ForUpload_0.pdf.

de SAA ou une obligation de tests rigoureux avant leur déploiement. Cette piste reste néanmoins sujette à débat, notamment en raison de la réticence de plusieurs grandes puissances à imposer des restrictions strictes sur ces technologies émergentes. Le droit international humanitaire repose actuellement sur l'idée qu'un humain doit être responsable d'un acte militaire. Or, dans le cas des SAA, si un dommage est causé, l'identification du responsable – concepteur, opérateur ou commandement militaire – peut devenir complexe. Un cadre normatif adapté pourrait établir une chaîne de responsabilité intégrant ces différents acteurs.

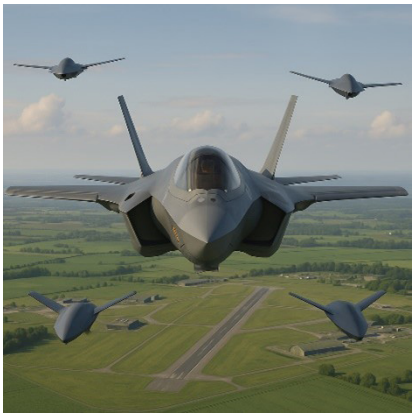


Illustration générée par l'IA

Au-delà de l'enjeu juridique, la question de la souveraineté se pose. Jusqu'à quel point la Belgique doit-elle dépendre d'acteurs étrangers pour ces technologies ? Aujourd'hui, elle ne développe pas de SAA de manière indépendante et dépend de fournisseurs étrangers. Une approche hybride pourrait être envisagée, combinant une participation active à des projets (de préférence européens) et un renforcement des capacités nationales dans des domaines clés comme la cybersécurité, la certification des algorithmes, le stockage des données et la réglementation. L'absence de cadre réglementaire international ajoute une autre dimension au problème. Lors du Sommet pour l'action sur l'IA – Enjeux de Défense (*AI Action Summit – Military Talks*) à Paris, le ministre français des Armées, Sébastien Lecornu, a souligné que la France souhaite anticiper et encadrer ces évolutions technologiques tout en garantissant un équilibre entre innovation et contrôle. Il a insisté sur la nécessité pour l'Europe de développer ses propres capacités en matière d'IA militaire afin de préserver son autonomie stratégique et d'éviter une dépendance excessive vis-à-vis des puissances étrangères. Cette vision rejoint les préoccupations belges concernant l'encadrement des SAA et la nécessité de garantir un contrôle humain significatif sur leur développement, leur déploiement et leur mise en œuvre.

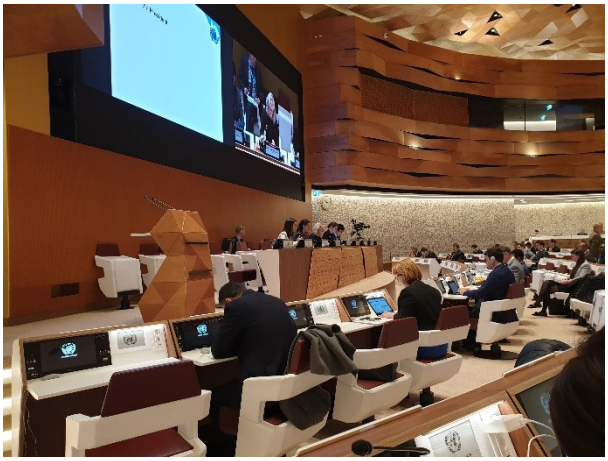
Un autre obstacle majeur à la réglementation des SAA réside dans l'absence d'une définition consensuelle. Cette absence complique la mise en place d'un cadre réglementaire efficace et cohérent car, sans définition précise, il devient difficile d'appliquer des normes juridiques claires et contraignantes.

Le Comité international de la Croix-Rouge (CICR)[6] a proposé une définition de travail des SAA, les décrivant comme des systèmes « capables de sélectionner et d'engager des cibles sans intervention humaine après leur activation ». Cette définition, volontairement fonctionnelle et centrée sur l'autonomie dans le processus de ciblage, vise à identifier les systèmes susceptibles de poser des problèmes juridiques et éthiques spécifiques au regard du droit international humanitaire.

Il convient toutefois de distinguer cette catégorie des autres systèmes militaires dotés de fonctions automatisées ou intelligentes, mais qui ne relèvent pas nécessairement du ciblage autonome au sens strict : systèmes à létalité partiellement autonome, aides à la désignation de cibles, effecteurs dépendants de l'intervention humaine pour l'engagement ou encore capacités défensives à réaction rapide comme les systèmes d'armes rapprochés (*close-in weapon systems*). Le débat actuel met ainsi en lumière la nécessité de catégorisations précises pour appréhender la diversité croissante des technologies d'armement intelligent.

Toutefois, cette définition ne fait pas l'unanimité. Certains États, notamment les grandes puissances militaires, considèrent que le degré d'autonomie varie considérablement selon les contextes d'utilisation et que la distinction entre armes autonomes, partiellement autonomes et automatisées reste floue. D'autres estiment qu'il est préférable de réglementer les effets de ces armes plutôt que de tenter de définir leurs caractéristiques techniques. Le CICR, tout comme la Belgique, insiste par ailleurs sur la nécessité d'un contrôle humain significatif, ce qui pose la question de savoir à quel niveau et à quel moment ce contrôle doit être exercé, sujet

[6] Un système d'arme autonome est un système qui, une fois activé, peut sélectionner et engager des cibles sans intervention humaine (voir CICR, *Position du CICR sur les systèmes d'armes autonomes*, 12 mai 2021).



© Dirk Naessens

sur lequel les divergences demeurent profondes entre les États. Le Groupe d'experts gouvernementaux sur les systèmes d'armes létaux autonomes (GGE LAWS) de la Convention sur certaines armes classiques (CCAC) des Nations Unies a tenté d'élaborer une définition englobant les systèmes capables d'agir sans intervention humaine immédiate, mais les discussions n'ont pas abouti à un consensus en raison des divergences entre États. Certains pays, comme la Belgique, la France et l'Allemagne, insistent sur la nécessité d'un contrôle humain significatif, tandis que d'autres, notamment les États-Unis et la Russie, estiment qu'une approche plus flexible est préférable. Pourtant, disposer d'une définition précise ou du moins d'une caractérisation de ces systèmes peut s'avérer précieux pour encadrer efficacement leur développement et leur utilisation. Sans consensus sur ce qu'est une arme autonome ou du moins sur ce qui la caractérise, il est difficile d'établir un cadre légal international applicable. Les États et les entreprises privées peuvent en outre interpréter à leur avantage l'absence de cadre défini, favorisant ainsi la prolifération de systèmes difficilement contrôlables. Certains experts estiment toutefois qu'une définition stricte des SAA n'est pas nécessaire, allant même jusqu'à prétendre qu'elle serait contre-productive. Une définition trop rigide risquerait de devenir obsolète rapidement, à mesure que les technologies évoluent et que les capacités des systèmes autonomes se diversifient. D'autres spécialistes suggèrent pourtant qu'il serait plus efficace de réglementer les effets de leur utilisation plutôt que leurs caractéristiques techniques, en s'appuyant sur des principes généraux du droit des conflits armés. L'absence de consensus international ralentit considérablement les discussions réglementaires et témoigne des approches divergentes entre États.

Parmi les aspects cruciaux à considérer figure la question de la licéité de ces systèmes, notamment au niveau des principes fondamentaux du droit des conflits armés, tels que la distinction entre combattants et civils, la proportionnalité et la nécessité militaire. Conformément à l'article 36 du premier protocole additionnel aux conventions de Genève, chaque État est tenu d'évaluer la conformité des nouvelles armes, moyens ou méthodes de guerre avec le droit international humanitaire avant leur adoption ou leur acquisition. Cette obligation pose un défi particulier pour les SAA, dont le comportement en situation réelle peut être difficile à prévoir, notamment en raison de leur capacité d'apprentissage et d'adaptation. En Belgique, cette évaluation est confiée à la Commission d'évaluation juridique des nouvelles armes, des nouveaux moyens et des nouvelles méthodes de guerre (CEJ), qui a pour mission de remettre un avis au chef de la Défense (CHOD) sur toute nouvelle arme, tout nouveau moyen ou toute nouvelle méthode de guerre en cours d'étude ou de mise au point par les forces armées ou sur toute arme que les forces armées souhaiteraient acquérir ou adopter. De plus, la nature dynamique de l'intelligence artificielle rend difficile la vérification de la conformité des systèmes sur le long terme : un algorithme évolutif pourrait aboutir à des comportements imprévus ou non conformes aux règles initiales. Ces incertitudes soulèvent des interrogations sur la manière dont les États peuvent effectivement remplir leur obligation de vérification et de contrôle, rendant indispensable un cadre d'évaluation technique et juridique adapté. Or, l'absence de cadre juridique spécifique aux SAA complique cette évaluation.

Les doctrines militaires doivent être adaptées pour inclure ces nouvelles capacités et réfléchir à la manière d'assurer une supervision humaine efficace. Bien que ces technologies offrent des avantages tactiques en matière de rapidité de réaction et de précision, elles posent aussi des défis logistiques et nécessitent une infrastructure technologique avancée. Une dépendance excessive aux SAA pourrait également engendrer de nouvelles vulnérabilités stratégiques. Ces technologies doivent par ailleurs être compatibles avec les engagements internationaux de la Belgique en matière de droit humanitaire. Comment garantir que ces systèmes respectent

les principes fondamentaux de distinction, proportionnalité et précaution en matière d'attaque ? Une réflexion approfondie sur leur encadrement juridique est indispensable. Le ministre français Lecornu a également rappelé, lors du Sommet pour l'action sur l'IA – Enjeux de Défense, l'importance d'un cadre réglementaire solide, affirmant que la France soutient une approche équilibrée où les avancées technologiques ne compromettent ni l'éthique ni la sécurité internationale. Cette prise de position illustre bien les défis auxquels les États européens sont confrontés : encourager l'innovation tout en respectant les principes fondamentaux du droit des conflits armés.

Enfin, la sécurisation des SAA' contre les cyberattaques constitue un enjeu critique, non pas tant du fait de leur connectivité intrinsèque, comparable à celle d'autres systèmes de combat modernes, que de leur capacité à prendre des décisions létales sans supervision humaine immédiate. Une attaque informatique réussie pourrait compromettre la logique décisionnelle embarquée, altérer la désignation de cibles ou détourner le système de sa mission initiale, avec des conséquences potentiellement irréversibles. La Belgique doit donc investir à la fois dans des technologies de supervision en temps réel et dans une doctrine d'emploi limitant les vulnérabilités systémiques.

Les discussions internationales sur les SAA mettent en lumière des divergences profondes entre les États. Les États-Unis et la Chine, engagés dans une course à l'innovation, développent activement ces systèmes avec une approche axée sur la supériorité technologique et le maintien d'un avantage stratégique. À noter que la Chine insiste lourdement sur le développement d'une définition précise des SAA. La Russie, quant à elle, se montre favorable à une intégration massive des SAA sur le champ de bataille et s'oppose à toute restriction significative pouvant limiter ses capacités militaires, considérant que les États doivent rester responsable de leurs SAA dans le respect du droit international humanitaire existant. Parmi les pays européens, les Pays-Bas soutiennent un instrument juridiquement contraignant pour encadrer le développement et l'utilisation des SAA, insistant sur l'importance

d'une régulation claire et efficace. L'Allemagne défend un contrôle rigoureux, insistant sur la nécessité d'un « contrôle humain significatif » dans les décisions létales. La France, pour sa part, adopte une posture intermédiaire : elle reconnaît l'intérêt stratégique des SAA tout en plaidant pour une régulation garantissant un rôle décisionnel humain.

Les armes autonomes constituent un défi en matière de sécurité et de droit international. Leur intégration dans les stratégies militaires mondiales présente à la fois des opportunités et des risques majeurs.

D'un côté, ces systèmes offrent des bénéfices significatifs. Ils permettent d'augmenter la rapidité de réaction face à des menaces, améliorant ainsi l'efficacité opérationnelle. Grâce à l'intelligence artificielle, ils peuvent traiter des volumes massifs de données en temps réel et prendre des décisions adaptées aux situations dynamiques du champ de bataille. L'automatisation de certaines tâches militaires réduit également le risque pour les soldats en limitant leur exposition aux zones de conflit. Si elle s'appuie sur des algorithmes rigoureusement calibrés et encadrés, l'autonomie pourrait en outre contribuer à une plus grande précision opérationnelle, en exploitant des flux de données multisources (capteurs, terrain, comportement cible) plus rapidement qu'un opérateur humain. Dans certaines conditions, cela peut réduire le risque de dommages collatéraux, à condition que le système soit déployé dans des environnements maîtrisés et respecte scrupuleusement les principes de distinction et de proportionnalité.[7]

Toutefois, ces avancées ne sont pas sans contrepartie. Si elles permettent d'améliorer la réactivité et la précision des opérations militaires, elles posent aussi des défis éthiques, juridiques, opérationnelles et sécuritaires. L'un des principaux dangers est la perte de contrôle humain. En dépit des efforts pour garantir un contrôle humain significatif, la complexité des algorithmes pourrait entraîner

[7] United Nations Institute for Disarmament Research (UNIDIR), *The Impact of Autonomy on the Law of Armed Conflict* (Genève : UNIDIR, 2021).

des décisions imprévues et difficilement explicables (*black box*, ou boîte noire), posant des dilemmes éthiques et opérationnels. Le risque de prolifération de ces technologies entre les mains d'acteurs non étatiques est également une source de préoccupation, notamment en raison de leur potentiel de détournement à des fins terroristes. C'est par ailleurs un élément que la Belgique a récemment remis sur la table lors du dernier GGE LAWS. Enfin, les menaces cybernétiques sont accrues avec ces systèmes, une manipulation malveillante pouvant transformer ces armes en instruments incontrôlables, exacerbant ainsi les conflits au lieu de les atténuer.

Une régulation efficace devra conjuguer réalisme stratégique et principes éthiques. Alors que la communauté internationale peine à s'accorder sur des règles claires, le développement et le déploiement de ces systèmes se poursuivent à un rythme soutenu. La Belgique, en tant que nation engagée sur la scène internationale, a choisi une posture adaptée pour ne pas subir les décisions prises par d'autres, tout en contribuant activement aux efforts visant à encadrer ces technologies émergentes. C'est la raison pour laquelle notre pays continue de s'engager activement dans les discussions du GGE LAWS en ne fermant pas la porte à une participation dans un processus qui pourrait mener à une interdiction/réglementation largement portée par la communauté internationale.

Mots-clés : autonomie, responsabilité, régulation/réglementation