

## ***Les nouvelles technologies militaires numériques et les systèmes d'armes autonomes***

*L'avenir de la guerre<sup>1</sup>*

### **Groupe de travail de la Fondation Friedrich-Ebert sur la politique de sécurité internationale**

- Il est urgent de mener des études scientifiques approfondies pour analyser les conséquences et les risques des nouvelles technologies militaires numériques pour la politique, la société et les forces armées. Le gouvernement allemand et le Bundestag devraient impérativement encourager ce type d'études afin d'élaborer des stratégies solides sur le plan politique et en mesure d'être acceptées par la société.
- Confier entièrement à des machines la décision de tuer des personnes est totalement inacceptable. Dans le cadre de l'UE et de l'OTAN, il faut parvenir à un accord visant à garantir de manière permanente l'autonomie de la décision humaine lors de l'utilisation de systèmes militaires numériques.
- Les applications militaires portées par le cyberspace, l'intelligence artificielle et l'autonomisation doivent faire l'objet d'un contrôle préventif et actif des armements au niveau international. L'Allemagne devrait assumer un rôle actif et porter le débat sur le contrôle des armements par des initiatives ciblées.
- Dans les Etats démocratiques, les décisions relatives aux capacités des forces armées et aux approvisionnements militaires sont soumises au contrôle parlementaire. Les conditions de ce contrôle doivent être réunies grâce à la compétence technique des députés sur ces questions.

---

Le groupe de travail sur la politique de sécurité internationale est un forum d'échange de la Fondation Friedrich-Ebert consacré aux sujets d'actualité de la politique de sécurité. Les membres de ce groupe de travail sont issus du Bundestag, des ministères fédéraux allemands et d'instituts de recherche.

En font notamment partie : Franz H. U. Borkenhagen, Michael Bröning, Hans-Georg Ehrhart, Tobias Fella, Helmut W. Ganser, Michael Hofmann, Alexander Kallweit, Anna Maria Kellner, Wulf Lapins, Marius Müller-Hennig, Detlef Puhl, Jürgen Schnappertz et Oliver Thränert.

---

<sup>1</sup> Une publication du département « analyse politique internationale » de la Friedrich-Ebert-Stiftung.

La révolution numérique apporte une évolution extrêmement rapide des systèmes d'information et de communication d'un nouveau genre – des systèmes qui nous facilitent la vie mais qui génèrent également de nouveaux risques. L'armement militaire et les processus militaires de planification et de commandement sont en profonde mutation. On développe de nouveaux systèmes d'armes qui vont conduire à moyen terme à révolutionner la conception de la guerre qui fonde encore aujourd'hui notre politique de sécurité et de défense. On voit poindre à l'horizon de nouvelles formes de guerre automatisées, voire autonomes, qui peuvent échapper au contrôle des humains et réduire à néant la liberté de choix d'une politique démocratique.

### **1. Dynamique du développement technologique : état des lieux et perspectives d'évolution**

En matière de développement de systèmes d'armes autonomes, les Etats-Unis et Israël disposent aujourd'hui d'une avance technologique et continuent d'être les moteurs de l'innovation. En 2014, le Pentagone a pris une nouvelle initiative en matière d'armement, la "Third Offset Strategy". Comme par deux fois déjà, dans les années 1950 et dans les années 1970, il s'agit de garantir la sécurité des Etats-Unis grâce à la supériorité technique. D'autres nations disposant d'une industrie de haute technologie, comme la France et la Grande-Bretagne, la Chine et la Russie, le Japon et la Corée du Sud, promeuvent également ces évolutions technologiques.

A l'automne 2014, le secrétaire d'Etat américain à l'approvisionnement, la technique et la logistique au Pentagone, Frank Kendall, a commandé une étude sur les problèmes scientifiques, juridiques, militaires et politiques qu'il faudrait résoudre pour pouvoir employer de nouvelles technologies numériques, y compris des systèmes autonomes, à tous les niveaux. Au sein de l'OTAN, plusieurs services se penchent également sur ces questions. Depuis bien longtemps, un débat animé s'est engagé entre spécialistes, en particulier aux Etats-Unis, sur les perspectives et les risques de cette évolution. En Allemagne, cette discussion, qui aujourd'hui encore peine à s'organiser, devrait être amplifiée de toute urgence. L'enjeu n'est pas seulement d'identifier les possibilités technologiques

déjà en cours de développement ou en passe de l'être. Il s'agit avant tout d'examiner en quoi les nouvelles technologies peuvent déterminer et éventuellement modifier notre action et donc notre capacité à concevoir une politique de sécurité.

Quelques exemples des développements en cours :

- L'évolution vers une mise en réseau complète de tous les domaines de l'existence ("l'internet des objets"), dans un espace mondial de données théoriquement illimité (le cyberspace) n'offre pas seulement des chances, mais aussi de multiples possibilités d'attaques contre les flux de communication (notamment les cyberattaques, les manipulations), qui pourraient avoir des conséquences incontrôlables et dévastatrices sur notre sécurité et notre capacité militaire à établir cette sécurité.
- Les nouveaux modes de production tels que l'impression 3D à partir d'une multitude de matériaux offrent non seulement aux "Etats voyous", mais aussi à des groupuscules ou à des particuliers la possibilité de produire des armes, de les doter d'équipements de haute technologie et de les utiliser, notamment à des fins terroristes.
- Depuis longtemps, le développement d'un nombre toujours croissant de fonctions dans des domaines d'application civils (par exemple, la voiture sans chauffeur) est également ouvert aux systèmes d'armes et de commandement militaire. Cette évolution pose des questions fondamentales sur les possibilités et les limites du contrôle par l'homme et sur la responsabilité humaine face à la destruction et à la mort.
- Le développement de technologies logicielles allant jusqu'à l'intelligence artificielle produit encore plus d'innovations dans tous les domaines de la vie, y compris dans le domaine militaire.

Tout ceci n'est plus de la "science-fiction", mais de la réalité en devenir. Dans ce contexte, le présent article se penche sur l'automatisation des systèmes militaires, sans négliger les conséquences technologiques pour l'ensemble du système politico-militaire. Il examine une série de questions fondamen-

tales, d'ordre politique, sociétal, juridique et également éthique. L'Allemagne, qui mène sa politique de sécurité et de défense exclusivement dans le cadre de l'Europe et des alliances, pourrait à l'avenir se retrouver en contradiction avec ses principaux partenaires. Il est nécessaire de mener un débat public sur la portée des conséquences de l'évolution technologique, afin que les bonnes décisions puissent être préparées, prises et assumées dans la durée.

### **Sur la voie de l'intelligence artificielle (IA) : les systèmes d'armes autonomes**

Dans sa forme la plus simple, l'autonomie est la capacité d'une machine – matérielle et logicielle – d'exécuter une tâche sans intervention humaine. Un système autonome est une machine qui, lorsqu'elle est activée, assume de façon autonome une mission ou une fonction.

Il est très difficile de parvenir à un consensus scientifique et politique sur les définitions et les caractéristiques des systèmes d'armes autonomes, tant le sujet est complexe. A ce jour, aucune définition universellement acceptée n'a pu être trouvée. Même la question de savoir s'il est nécessaire de trouver des définitions exactes pour pouvoir organiser le contrôle des armements est sujette à controverse. Le présent article s'appuie sur les définitions de travail suivantes, qui reposent largement sur les concepts employés par le Pentagone :

- Un *système d'armes autonome* est un système d'armes qui, lorsqu'il est activé, peut sélectionner et engager des cibles sans qu'il soit nécessaire / possible pour un opérateur humain d'intervenir.
- Un *système d'armes autonome supervisé* est un système d'armes qui offre à l'opérateur humain la possibilité d'intervenir et de refuser certaines actions, telles que l'engagement des armes.
- Un *système d'armes partiellement autonome* est un système d'armes qui, lorsqu'il est activé, peut engager une cible ou un groupe particulier de cibles qu'un opérateur humain a préalablement sélectionnés et autorisés pour l'attaque.

En réalité, l'automatisation, phase préalable à l'autonomie, est déjà utilisée pour une mul-

titude de tâches militaires. Nombre d'entre elles sont directement ou indirectement liées à l'emploi des armes. C'est notamment le cas de l'identification, la poursuite, la priorisation et le marquage de cibles, le choix de l'instant auquel l'arme est déclenchée et l'instant de l'impact. Au moins 30 pays disposent de systèmes plus ou moins automatisés ayant des fonctions autonomes supervisées par des opérateurs humains. Ces systèmes sont notamment employés pour protéger les personnels dans les infrastructures militaires et sur les bâtiments de la marine, puisque les délais de réaction des humains ne sont pas suffisants pour cela. Les principaux acteurs du développement de systèmes d'armes autonomes défensifs, et aussi de plus en plus offensifs, sont les Etats-Unis et Israël, la Chine, le Japon et la Corée du Sud, ainsi que la Grande-Bretagne, la France et la Russie. Le préalable à ces développements est une industrie de haute technicité et performante technologiquement.

Dans ce cadre, on développe sans cesse des algorithmes plus complexes qui mettent les machines en capacité de prendre des décisions de façon autonome. Cela débouche sur de nouveaux scénarios d'engagement, encore plus complexes. Par ailleurs, les progrès accomplis dans le domaine des capteurs rendent les systèmes d'armes du futur encore plus performants. On peut notamment citer la très forte amélioration de la distinction ami/ennemi et de la reconnaissance de cible. S'y ajoutent une meilleure mise en réseaux des machines (fonctionnant en "essaim") et une plus grande maturité des interactions entre l'homme et la machine. Ces évolutions sont portées par les progrès du développement logiciel dans le domaine de l'intelligence artificielle.

### **Sur la voie de l'intelligence artificielle : les systèmes de commandement et de planification**

Nous sommes visiblement au début d'une évolution dynamique dans laquelle les systèmes logiciels seront de plus en plus capables d'apprendre et de générer automatiquement des programmes informatiques. Dans quelques décennies, l'intelligence artificielle pourrait peut-être atteindre et même dépasser les performances cognitives des cerveaux humains. Associée à la généralisation des réseaux numériques (l'internet des objets), l'intelligence artificielle va s'immiscer

dans pratiquement tous les domaines de l'économie et de la société et vraisemblablement produire des bouleversements socioculturels considérables. Cette évolution représente des chances formidables, mais aussi des risques considérables. A l'ouverture d'une conférence internationale sur l'intelligence artificielle en 2015 à Buenos Aires (l'International Joint Conference on Artificial Intelligence - IJCAI), de nombreux chercheurs de réputation internationale dans le domaine de l'intelligence artificielle ont publié une lettre ouverte dans laquelle ils mettent en garde contre les risques considérables inhérents aux armes autonomes sans véritable contrôle humain effectif.

Selon ces auteurs, les armes autonomes pourraient déjà être employées dans quelques années, et non dans quelques décennies. Ils les décrivent comme la troisième révolution dans la conduite de la guerre, après la poudre à canon et les armes nucléaires.

Compte tenu du fait que la révolution numérique va se poursuivre, l'enjeu sera de concevoir et piloter les applications de l'intelligence artificielle de sorte que l'autonomie de décision des humains ne soit pas remise en question d'une manière générale. Cela implique le cas échéant des actions et des technologies destinées à endiguer ou à réguler l'intelligence artificielle pour se prémunir en particulier contre des débordements incalculables ou des sauts qualitatifs ("l'explosion d'intelligence").

Les nouvelles technologies numériques vont également percer dans le domaine de la politique militaire et de sécurité et entraîner au fil du temps des bouleversements considérables. Pour autant, on ne sait pas encore grand-chose du développement de logiciels de soutien à la planification stratégique et au commandement d'opérations dans les nations ayant de hautes capacités technologiques. Il s'agit dans un premier temps des armes stratégiques, en particulier des domaines de l'alerte précoce, de la défense antimissile et de la dissuasion nucléaire. Mais au-delà, l'intelligence artificielle pourrait trouver des applications dans les systèmes d'information et de commandement stratégique (Command and Control), les systèmes de communication, de navigation, de renseignement et de surveillance ainsi que dans tout le domaine des capacités défensives et offensives dans le cyberspace, dont elle pourrait améliorer l'efficacité. Les fonctions

autonomes pilotées par l'intelligence artificielle représentent une évolution plus grave dans ces domaines que dans celui des systèmes d'armes tactiques, dans la mesure où ces fonctions autonomes agissent directement sur les capacités de contrôle politique de l'engagement des forces armées.

De même, les supercalculateurs pourraient bien faire tôt ou tard leur entrée dans le domaine essentiel des analyses politico-stratégiques et des processus de décision, à l'échelon national et multinational. Cela correspond à la logique de l'évolution technologique bien qu'on ne dispose pas encore d'analyses scientifiques sur ces sujets. L'un des moteurs essentiels de cette évolution pourrait bien être le raccourcissement des délais de prise de décision, qui est la résultante de l'accélération des événements qu'entraîne la technologie dans les conflits armés.

On observe dès à présent les premiers signes de ces évolutions : au Pentagone, une directive interne portant sur "l'étude d'autonomie menée par le conseil scientifique de la défense en 2015" (Defense Science Board 2015 Study of Autonomy), évoque expressément le supercalculateur Watson d'IBM et examine la possibilité d'utiliser des aides automatiques à la décision et des systèmes de planification automatiques. Selon son constructeur IBM, le programme Watson est un système informatique cognitif, capable dès à présent non seulement de comprendre le langage naturel, mais aussi de traiter des informations linguistiques et de formuler en langage naturel des réponses précises aux questions qui lui sont posées.

Watson pourrait ainsi être un exemple de ces machines super-intelligentes qui seront tôt ou tard utilisées dans les prises de décision politiques et militaires. Etant donné la nécessité de collecter des quantités toujours plus importantes de données dans des délais toujours plus courts, de les stocker et de les analyser pour en tirer des conclusions, l'utilisation de ces machines est appelée à progresser de manière inéluctable. Par ailleurs, ce processus va nécessiter toujours plus d'énergie, de sorte que la vulnérabilité de ce type de systèmes, tributaires d'une alimentation électrique protégée, aura également tendance à s'accroître.

Il ne fait aucun doute que les architectures de supercalculateurs sont destinées à devenir des systèmes d'assistance ou de recom-

mandation, dont l'utilisation ne doit en rien diminuer l'autonomie de décision des opérateurs humains. Dans la pratique, le risque est néanmoins grand de voir insidieusement s'installer chez les personnes qui les utilisent une dépendance et une accoutumance aux supercalculateurs dans le processus de prise de décision. Les ordinateurs ultra-performants permettront dans certaines circonstances de simuler la réalité dans des scénarios de crise, d'établir des prédictions sur le comportement des divers acteurs impliqués et participeront ainsi à la prise de décision. Cela pose...

### ... une série de questions critiques :

Par exemple, est-ce que la dépendance à l'égard des données et des solutions proposées par les ordinateurs ne conduit pas inéluctablement à une incapacité à agir en cas de défaillance partielle ou totale des systèmes numériques ? Les acteurs aux niveaux du commandement politico-stratégique et militaire seront-ils encore en mesure, en cas de défaillance des systèmes numériques, de plantage des ordinateurs ou de coupure électrique généralisée, d'agir efficacement sans les aides numériques à la communication, la navigation et la prise de décision ? Il serait important d'y réfléchir, notamment dans la perspective d'éventuelles réactions asymétriques à une guerre numérique. Quelles seraient les conséquences des actions et des réactions en temps de crise et de guerre, si les deux parties utilisaient des analyses informatiques et des programmes informatiques d'aide à la décision ?

Ou encore : à quel niveau faut-il estimer le risque que les responsables politiques, les hauts fonctionnaires ou les militaires de l'état-major en viennent à croire qu'ils prennent leurs décisions de façon libre et indépendante, alors qu'en réalité ils n'agissent plus que sur la base d'une réalité simulée générée par des ordinateurs et selon des options d'action préfabriquées ? Seront-ils alors encore capables de s'apercevoir que l'intelligence artificielle leur impose leurs choix, après s'être progressivement habitués aux conseils de ces nouvelles machines intelligentes, avec de bons résultats pendant un certain temps ?

Les décisions politiques et militaires ont de tout temps été prises en s'en remettant pour une part essentielle à l'intuition. En d'autres termes, elles ont été prises sur la base d'un

jugement global fondé sur l'expérience et qui va bien au-delà d'une démarche purement cognitive. Les décideurs au sein des gouvernements et des commandements militaires disposeront-ils encore de cette intuition saturée d'expérience, de ce "savoir ressenti", si leur pensée est de plus en plus conforme au fonctionnement d'un ordinateur, si "l'humanisation" des machines a pour corollaire une "machinisation" des humains (Schirrmacher) ? Quelles sont les conséquences sur les situations de crises urgentes dans lesquelles il faut immédiatement décider d'employer la force militaire, c'est-à-dire de faire la guerre – ou pas ?

Ces questions se justifient-elles ou bien relèvent-elles plutôt, aujourd'hui encore, du domaine de la science-fiction ? La politique peut-elle se permettre de piloter à vue dans ce domaine et d'attendre de voir, parce que les systèmes intelligents n'existent pas encore, ou seulement à un état rudimentaire ? L'état actuel apparent de la recherche, y compris en Allemagne, et le fait qu'un large débat critique et prospectif a déjà été engagé aux Etats-Unis sur l'intelligence artificielle sont autant d'éléments qui témoignent d'un besoin concret d'agir et de traiter la question.

Le développement et l'emploi de calculateurs super-intelligents dans le domaine de la politique de sécurité doivent impérativement s'accompagner de mesures actives d'évaluations et de mesures garantissant la maîtrise de ces nouvelles technologies par l'homme. L'histoire nous enseigne qu'il n'y a jamais eu de véritable contrôle de l'émergence de nouvelles technologies. C'est toujours a posteriori que les effets des bonds technologiques, qu'ils soient positifs ou négatifs, ont été constatés. Ce fut le cas pour la physique nucléaire du XXe siècle, qui a permis la construction des bombes atomiques, ou pour le développement de l'internet, qui n'a pas suscité de débat sur la sécurité des réseaux au départ. Au XXIe siècle, tout l'enjeu sera de ne pas tomber dans le piège des nouvelles technologies dans lequel l'action politique, dont le mode de fonctionnement consiste à réparer les dégâts a posteriori, se laisse habituellement enfermer.



## 2. Les conséquences politiques et stratégiques

Les systèmes d'armes sont par définition conçus pour la guerre. Cependant, la politique a pour ligne directrice d'éviter ou de prévenir la guerre, de dissuader les agresseurs et, seulement lorsque l'option de la dissuasion est épuisée, d'être en mesure de faire la guerre et de remporter la victoire. De ces éléments découlent une série de questions fondamentales :

- Le développement et la mise en service dans nos forces armées de systèmes d'armes automatisés, puis de systèmes d'armes autonomes, peuvent-ils déboucher insidieusement sur une dynamique propre de la technique dans la conduite de la guerre ?
- Cette évolution serait-elle conciliable avec la notion de responsabilité reposant sur la légitimité démocratique ? Ou bien l'autonomie de décision de la politique risque-t-elle d'être de plus en plus restreinte ? Dès lors, en quoi consisterait précisément cette restriction du contrôle politique ?
- Pourrait-elle conduire à une perte du contrôle politique dans les situations de guerre et de conflit ? Et comment préserver l'autonomie de décision et le contrôle politique face à une automatisation croissante de l'action militaire ?

Les développements technologiques présentés permettent d'imaginer certaines hypothèses pour le déroulement des opérations de guerre, qui pourraient radicalement modifier, voire tendre à supprimer au moins partiellement le rôle des opérateurs humains responsables, alors que ce rôle est capital, en particulier lorsqu'il est question de vie ou de mort.

La question centrale est donc d'identifier les conséquences de ces développements technologiques sur notre vision de la guerre et sur nos capacités à la faire et de trouver les solutions pour garantir un contrôle politique démocratique permanent. Cela implique l'organisation d'une responsabilité entre les hommes, qui doit impérativement être placée sur un plan éthique et qu'il convient d'assumer concrètement.

## Les conséquences pour la politique de sécurité

Du point de vue de la sécurité, le fait qu'un pays dispose d'un nombre suffisant de systèmes d'armes autonomes pourrait l'amener à choisir plus facilement d'intervenir militairement dans la mesure où le risque pour la vie de ses soldats - et les coûts de l'intervention - serait réduit; Par voie de conséquence, il lui serait d'autant plus aisé de justifier ses décisions vis-à-vis de son opinion publique.

Les évolutions technologiques posent aussi des défis considérables en matière de contrôle international des armements. Dans l'hypothèse d'une poursuite de l'évolution technologique, allant vers des armes toujours plus rapides, plus performantes et qui deviendraient autonomes, quelles seraient les conséquences sur les traités existants en matière de contrôle des armements et sur l'élaboration de nouveaux accords qui tiendraient compte de ces évolutions technologiques ? La mise en route d'un pilotage coopératif et préventif du contrôle de ces armements pourrait passer par la signature d'accords destinés à garantir la plus grande transparence possible et par l'élaboration d'un code de conduite. Pour ce faire, des mesures instaurant un climat de confiance et des procédures de vérification sont indispensables. Est-ce de cette manière que l'on pourra éviter une course effrénée aux armements entre les pays de haute technologie ?

Peut-on éviter que les nouveaux systèmes d'armes ne tombent dans de mauvaises mains, que ce soient ou non celles d'un pouvoir étatique ? Quelles sont les conséquences possibles de cette évolution sur d'autres domaines de la sécurité, comme les forces de police et la protection des frontières, et quelles seraient les conséquences sur l'équilibre délicat entre sécurité et liberté ou entre sécurité intérieure et extérieure ? Ces évolutions entraînent donc de véritables choix de société.

## Les conséquences en termes d'alliances

La politique de sécurité de l'Allemagne s'inscrit dans le cadre de l'UE et de l'OTAN. De ce fait, il est très important de savoir comment nos alliés traitent ces questions. Leurs points de vue à l'égard du développement et du

rôle des systèmes d'armes autonomes sont néanmoins très différents. D'une part, aucun Etat n'approuve jusqu'à présent le développement et l'emploi de systèmes d'armes autonomes capables de fonctionner sans aucun contrôle humain. D'autre part, les Etats-Unis, notamment, continuent de travailler au développement de systèmes d'armes autonomes. Certes, ces travaux intègrent la nécessaire garantie d'un "contrôle humain adéquat" mais il est bien difficile de savoir ce que cette formulation signifie précisément. Une chose est sûre : l'Allemagne a fortement intérêt à ce que la manière d'appréhender ce sujet soit définie par des règles compatibles avec le fonctionnement des alliances. En effet, il faut que nos forces armées soient interopérables et le demeurent. Que ce soit dans le cadre de l'UE ou dans celui de l'OTAN, tous les Etats membres sont des démocraties et font face aux mêmes problèmes de responsabilité démocratique à l'égard des systèmes d'armes autonomes. Des façons de procéder qui seraient différentes ou non concertées pourraient donc entraîner des problèmes politiques considérables dans le cadre de la coopération et donc pour la cohésion de l'alliance à long terme.

### **Les conséquences au regard du droit international**

Tout développement et toute utilisation d'armes, dont les systèmes d'armes autonomes, doit respecter les principes du droit international. Il s'agit des principes de distinction entre combattants et non-combattants, autrement dit entre soldats et civils, de proportionnalité des moyens engagés, de nécessité militaire et de réciprocité (respect des normes du droit international) ainsi que d'évitement des souffrances inutiles. En vertu de quoi, la Birmingham Policy Commission, un groupe d'experts composés de décideurs politiques britanniques et de chercheurs de l'Université de Birmingham, est arrivée à l'automne 2014 à la conclusion qu'il ne sera pas possible de développer des systèmes d'armes autonomes compatibles avec le droit international de la guerre. Dans une étude publiée en juin 2015 par la Fondation Friedrich-Ebert, Robin Geiss, spécialiste du droit international, arrive à la conclusion que les "décisions critiques" (notamment sur les questions de vie ou de mort) ne doivent pas être déléguées à des systèmes entièrement autonomes.

### **Les conséquences normatives et morales**

Compte tenu de notre système de valeur basé sur la dignité humaine (l'homme comme sujet de responsabilité), les décisions de recours aux armes mortelles ne peuvent en aucun cas être déléguées à des machines, même si celles-ci sont programmées et utilisées par des hommes. L'emploi de la force militaire doit être déclenché par une action volontaire dont un être humain doit être responsable. La guerre ne doit pas être menée "en pilotage automatique". Ainsi, la question fondamentale est de savoir si la responsabilité de décider de la vie ou de la mort peut être transférée à des algorithmes informatiques, sans qu'un humain n'ait au moins à en assumer la coresponsabilité et que les conséquences de ces actes pèsent sur sa conscience. La question posée est celle de la responsabilité, de la décision prise en conscience et des conséquences à assumer. Quelle forme prendrait par exemple la responsabilité en cas d'erreur, si l'emploi des armes n'était pas commandé par un commandant militaire à un soldat placé sous ses ordres, mais par un programmeur / opérateur ayant fourni au système d'armes un logiciel de combat ? Comment garantir une responsabilité assumée en cas de dommages collatéraux résultant d'un défaut de fonctionnement d'un robot de combat ? Doit-on, a-t-on tout simplement le droit de concevoir une telle interface entre l'homme et la machine qui serait porteuse de mort ? Cela vaut aussi pour l'éthique actuelle du commandement militaire, dont des systèmes d'armes autonomes pourraient s'affranchir. Les officiers ne donneraient plus leurs instructions et leurs ordres à des soldats placés sous leur responsabilité hiérarchique, mais à des experts informatiques en uniforme, qui confieraient au programme d'un système d'armes une mission que ce système d'armes exécuterait de façon autonome.

Par la suite, cette question se poserait avec encore plus d'acuité dans le cas de systèmes encore plus avancés, capables de prendre en charge des choix tactiques de missions complexes.

### Les conséquences économiques

A ceci s'ajoute un niveau économique : la technologie sur laquelle reposent les systèmes d'armes autonomes est avant tout développée à des fins civiles. Les universités et les entreprises travaillent depuis longtemps sur le développement de robots capables d'opérer de façon autonome dans le domaine civil et fonctionnant à l'aide de l'intelligence artificielle. Les intérêts en jeu, en termes de valorisation de cette technologie, sont énormes, comme en témoigne la discussion autour de la voiture sans chauffeur. C'est le secteur civil qui est le véritable moteur du développement économique, lequel se diffuse dans le secteur militaire, et non l'inverse. Le lien étroit entre le développement de ces technologies, effectué essentiellement par des entreprises privées, et les exigences de sécurité imposées par une utilisation militaire fait qu'il est nécessaire d'accorder une attention particulière à la divergence persistante entre les intérêts des uns et des autres : les entreprises technologiques fonctionnent selon un modèle économique qui vise souvent à une présence la plus rapide possible sur les marchés mondiaux. Les gouvernements et les organisations internationales portent une responsabilité sociale et politique, avec la plupart du temps un objectif national qui est d'établir des normes de sécurité élevées. Jusqu'à présent, il a déjà fallu trouver un point d'équilibre entre ces intérêts divergents. Or les marges de manœuvre de la politique en matière de décision pourraient être plus réduites que prévues et se retrouver à un niveau dont on ne saurait plus répondre, en raison de la vitesse à laquelle progressent ces développements.

### 3. Conclusion

Le développement de technologies militaires entièrement nouvelles est en marche, avec en ligne de mire la création de systèmes d'armes autonomes. Comme c'est le cas pour toute nouvelle technologie, ce processus comporte des chances et des risques. Il ne saurait être question de condamner par principe le recours au numérique et aux outils d'autonomisation dans le domaine militaire. Il s'agit de promouvoir l'utilisation légitime de la numérisation et d'endiguer par l'adoption de règles d'éthique et de droit international ses éventuelles conséquences négatives sur l'autonomie de décision des

êtres humains. Ainsi, des systèmes autonomes pourraient parfaitement s'avérer utiles dans le domaine des secours d'urgence et de la défense antiaérienne et antimissile : pour protéger la vie.

Cette évolution entraîne de vastes conséquences politiques, et même philosophiques et morales, qui vont bien au-delà de la politique de sécurité et de défense et jouent un rôle considérable dans l'élaboration de nos choix de société. Dans une société démocratique, ces questions doivent absolument faire l'objet d'un débat public. Les organes de planification de la défense de l'OTAN et de l'Union européenne, mais aussi les débats autour du Livre blanc du gouvernement allemand sur la politique de sécurité, l'élaboration de la nouvelle stratégie européenne de sécurité de l'UE et la rédaction du prochain concept stratégique de l'OTAN doivent être utilisés pour organiser ce débat. L'objectif du présent article est d'inciter et de contribuer à cette discussion.

L'opinion exprimée dans cette analyse n'engage pas nécessairement la position de la FES

Responsable de la publication :  
Stefan Dehnert, directeur du bureau parisien de la FES

**Publications à télécharger sur le site**  
[www.fesparis.org](http://www.fesparis.org):

[L'Union européenne de l'énergie : Un simple mot d'ordre ou une étape importante de l'intégration européenne?](#)  
par Georg Zachmann

[More Union in European Defence](#)  
Centre for European Policy Studies (CEPS) and Friedrich Ebert Stiftung (FES)

[L'UE et les pays de l'Est en 2030](#)

Quatre scénarios possibles des relations entre l'Union européenne, la Fédération de Russie, et leurs voisins communs  
par le **Groupe de planification "Scénarios EU+Est 2030"**