CID – MARS – FORUM DU FUTUR

COMPTE RENDU DU COLLOQUE

« NOUVELLES TECHNOLOGIES ET ART DE LA GUERRE »

LES TECHNOLOGIES INNOVANTES

Ecole Militaire – 28 avril 2004

LES TECHNOLOGIES INNOVANTES

Président : Jean-Louis GERGORIN, Vice-Président Coordination stratégique - EADS

Vice Amiral d'Escadre (cr) Jean BETERMIER – Vice-Président du Forum du Futur
Par délégation, j'ai la lourde responsabilité de lancer la troisième table qui portera sur les technologies innovantes. C'est un sujet difficile, risqué. Après avoir ce matin passé en revue les tendances qui peuvent se dégager des nouveaux types de conflits, les possibilités que nous offre une industrie de haut niveau dans l'espace, dans les télécommunications, dans les armes de précision, il convient de s'interroger sur l'avenir. La principale cause des grands échecs militaires est que l'on a toujours tendance, au nom des leçons de l'Histoire, à préparer le dernier conflit. Il nous paraissait donc important, ainsi qu'à votre directeur, de lancer une réflexion sur ce qui pourrait arriver dans les vingt prochaines années et qui serait de nature à déranger, à changer, à conduire à des ruptures et à une remise en cause des résultats des situations acquises.

Pour présider cette table, vous aurez le privilège d'avoir Jean-Louis GERGORIN qui est un stratège international de haut niveau. On lui doit en particulier la concentration d'une grande partie de l'industrie européenne de défense, ceci dans une grande optique de services à la Nation et à l'Europe. Nous avons réuni autour de cette table l'amiral TANDONNET qui est chargé d'imaginer l'avenir vu de l'EMA ; mon ami le Professeur BERCHE qui est le Doyen de Necker et un biologiste réputé ; le Professeur CAPPY qui est l'homme des nanotechnologies et des micro-systèmes ; l'ingénieur général FAYARD qui abordera le sujet sensible de la vulnérabilité des systèmes d'information aux différentes formes de menaces ; Monsieur Claude GUET qui est le directeur scientifique de la DAM. Monsieur Jacques BATTISTELLA, président de la CILAS, ayant eu un empêchement, Monsieur GUET a accepté avec la prudence, l'honnêteté et la rigueur qui caractérisent un scientifique de très haut niveau de prendre en compte une partie de la réflexion sur les lasers.

Attentes de l'EMA

Jean TANDONNET, secrétaire général du Collège des officiers de cohérence opérationnelle, EMA
Si vous me le permettez, j'exprimerai le sujet des technologies innovantes sous la forme suivante : quelles technologies innovantes nous paraissent prometteuses au regard des capacités opérationnelles ? Car l'objectif, au moins pour nous, militaires, est bien d'assurer de manière pérenne la sécurité de notre pays, de nos concitoyens, de notre continent et non de promouvoir la recherche. Cette question est essentielle pour le secrétaire général du collège des Officiers de Cohérence Opérationnelle (OCO) qui est en charge de la prospective à l'état-major des armées. Je n'aurai cependant pas la prétention d'y répondre en quelques minutes. J'aimerais cependant vous faire part de quelques réflexions.

Il est difficile de prévoir les menaces que nous aurons à affronter dans dix, quinze ou vingt ans. Nous savons qu'elles iront sans doute en se diversifiant et les événements du 11 septembre 2001 le laissent présager. Faute de prévoir l'imprévisible, il nous faut donc lui laisser le moins d'espace possible. Pour autant nous n'avons pas le droit

d'exclure un regain de difficultés dans les relations internationales pouvant se traduire par des tensions majeures entre puissances régionales. Ainsi, quelle que soit la nature des conflits et même si l'émergence de nouvelles menaces dissymétriques peuvent faire évoluer cette notion, un pays qui possède l'avance technologique - et nous en avons la prétention - sera toujours en situation de force.

Pour parler des technologies innovantes, permettez-moi de commencer par aborder la démarche prospective de la défense qui s'articule autour du plan prospectif à trente ans. Ce document, élaboré conjointement par la DGA et l'état-major des armées, guide notre stratégie de préparation du futur et permet de mieux préparer les décisions sur les plans d'équipements des armées. Il a pour but d'examiner les horizons nouveaux et de montrer les voies possibles. Notre mandat est de faire débuter à temps – ce terme est essentiel car trop tard ne sert à rien – les travaux dont les résultats permettront de faire les bons choix au bon moment, aussi bien pour lancer les programmes futurs que pour adapter les doctrines militaires comme les organisations. À ce titre, il permet d'identifier les technologies innovantes et les ruptures à venir pour être bien entendu au rendez-vous des échéances majeures.

Sans trop entrer dans les détails, je souhaiterais vous présenter, à titre d'exemple, quelques sujets qui paraissent importants à l'état-major des armées mais la liste est loin d'être exhaustive. Tout d'abord, sans empiéter sur ce que dira l'ingénieur général FAYARD, les technologies de l'information et de la communication sont un véritable défi global et non pas uniquement militaire. C'est la problématique de la mise en réseau de l'ensemble des informations avec un accès de plus en plus ouvert. Le corollaire est une augmentation permanente des besoins en débit. Je retiens deux techniques innovantes :

- la technique ultra large bande qui pourrait trouver des applications dans le monde militaire si ses performances sont confirmées ;

- la radio-logicielle, encore plus importante à mes yeux.
  Un même poste de radio est capable d'accueillir plusieurs formes d'ondes qui sont définies sous forme logicielle. Cela reste encore une problématique militaire et j'espère que cela pourra déboucher à court terme.

Ce sont sans doute, pour nous, des manières de résoudre la problématique très importante de l'interopérabilité, au moins de l'interopérabilité entre nos armées et même sur le plan international. Enfin, la mise en réseau sera conditionnée par l'utilisation des technologies IP issues d'Internet. Je répète que l'un des principaux challenges auxquels nous serons confrontés sera la capacité à extraire, pour chacun des acteurs, l'information pertinente le concernant - uniquement celle-ci - et de la lui faire parvenir.

Un autre sujet s'y rapporte : le renseignement. Pour maîtriser le renseignement, l'accès à l'espace des communications est un fait bien connu mais il faudra savoir faire face à l'augmentation énorme de la quantité d'informations recueillies et donc à la dilution de l'information pertinente. Cela se traduira par le développement de l'automatisation du traitement des informations au travers des techniques d'aide informatique à la recherche d'informations et de fusion de données multi-capteurs temps réel. En conséquence, le premier défi en matière d'observation et de

renseignement pour les années à venir concerne la maîtrise de l'évolution des moyens informatiques permettant d'intégrer toutes les sources d'informations.

Dans un domaine qui s'en rapproche, je citerai la lutte informatique qui va devenir de plus en plus essentielle pour la défense. La précision des armes et leur létalité mais également, à l'inverse, leur non-létalité sont également importantes. Le spectre des opérations dans lequel nous pourront être engagés, notamment dans le cas de la gestion de crise et en particulier du contrôle des mouvements de foule, comme nous l'avons souvent vécu au Kosovo, nous impose de disposer d'une gamme d'armements très diversifiée et aux effets différenciés. Dans ce domaine, je me permettrai un aparté sur la navigation. Les accéléromètres à poutres vibrantes et le gyromètre à résonateur hémisphérique seront certainement un facteur d'évolution sensible car leur architecture à l'état solide (c'est-à-dire sans pièces mécaniques en mouvement) leur confère un très haut potentiel de performance et de robustesse mécanique. Enfin, ces technologies atteignent des performances comparables à celles actuellement en service sur les accéléromètres pendulaires secs ou les gyromètres mécaniques et gyrolasers.

L'enjeu principal concernant l'avenir de la guerre optronique est le développement ou la maîtrise de l'accessibilité des sources laser en basse, moyenne et haute énergie. Pour les applications laser de basse énergie (brouillage ou neutralisation de fonctions optroniques pointées), les progrès sont continus. Pour le reste, c'est certainement plus difficile et on peut se demander si c'est à l'échelle de l'Europe. Les sciences de la vie et la protection de nos personnels face aux menaces radiologiques, chimiques et maintenant biologiques liées à un nouveau terrorisme dépasseront la sphère des armées. Je laisserai le Professeur BERCHE s'étendre sur ce sujet qu'il maîtrise beaucoup mieux que moi.

Je soulignerai simplement notre problématique, en tant que militaires, de l'ergonomie de ces équipements et du maintien du niveau opérationnel du combattant qui restera un enjeu primordial. Les protections actives de nos bateaux, aéronefs ou blindés mais également les protections passives comme la furtivité ou le leurrage reposeront sur les progrès continus que feront les matériaux métalliques et les matériaux composites. On peut vraisemblablement s'attendre à l'émergence de trois types de nouvelles solutions en termes de matériaux :

- les matériaux nanostructurés ;
- les biomatériaux comme, par exemple, les soies d’araignées ;
- les matériaux intelligents.

Dans le domaine du combat de contact, le principal enjeu technologique concerne l'augmentation du nombre d'équipements électroniques composant l'équipement du futur fantassin. Si l'on ne veut pas transformer le fantassin du futur en un bibendum incapable de se mouvoir, deux voies de progrès sont indispensables : l'utilisation de moyens portatifs de stockage de l'énergie électrique (peut-être des piles à combustible portatives d'ici dix ou quinze ans) et la capacité de transmission de données sans fil entre ces moyens électriques.

J'arrêterai là ces quelques pistes de réflexion en insistant à nouveau sur la nécessité de peser le degré de maîtrise technologique à posséder, notamment dans le cadre de notre besoin d'autonomie décisionnelle nationale et européenne.

Ma conclusion est une réflexion plus générale sur la prospective de défense. Le principe de la course aux armements tel que nous l'avons connu au siècle dernier semble avoir laissé la place au défi de la maîtrise des armements. Depuis quelque temps, ce ne sont plus les guerres qui poussent au développement des sciences mais plutôt les technologies nouvelles qui font émerger des systèmes militaires nouveaux. Ces derniers ne doivent pas systématiquement se substituer à leurs prédécesseurs mais répondre effectivement à des besoins opérationnels concrets et c'est tout l'enjeu de l'approche dite capacitaire. La problématique est donc de nous permettre de disposer soit des technologies innovantes, soit, plus simplement, d'éléments de choix sur des architectures possibles des futurs systèmes de défense. Le fruit ne doit pas être considéré isolément, il doit être le produit d'une réflexion qui intègre également l'évolution de la société et de l'environnement économique. C'est donc cette dynamique globale, et non pas la seule technique, qui peut créer des ruptures. Ainsi les nouvelles technologies de l'information et de la communication n'ont pas fini de révolutionner nos façons de faire. Les microtechnologies et les nanotechnologies sont porteuses de nouvelles ruptures et les biotechnologies progressent sans que soient résolus les problèmes éthiques qu'elles soulèvent. Elles nous rappellent en tout cas que l'homme est et restera toujours au cœur des systèmes mais nul n'en doute ici. Je vous remercie.

Jean-Louis GERGORIN
Je souhaite passer la parole au Professeur BERCHE pour parler d'un sujet qui risque malheureusement de devenir de plus en plus sensible, celui du risque que représente l'évolution des biotechnologies en termes de sécurité et de défense. Celles-ci ont de nombreux aspects positifs sur le plan de la santé publique mais ont également, malheureusement, des conséquences négatives sur le plan de la sécurité. Je demande donc au Professeur BERCHE, qui est membre du Conseil scientifique de la défense, de nous présenter ce sujet.

Biologie et biotechnologies

Patrick BERCHE, chef du service Bactériologie et Virologie de l'Hôpital Necker
Je remercie l'amiral BETERMIER de m'avoir invité. Je me focaliserai sur les armes biologiques et sur l'apport négatif des biotechnologies pour créer des armes nouvelles. Depuis deux ans, un certain nombre d'événements nous conduisent à avoir quelques sujets de crainte.

(Le Professeur BERCHE projette des transparents.)

Les armes biologiques sont des agents pathogènes que l'on utilise depuis le début de l'ère pasteurienne, depuis que l'on sait isoler des agents infectieux pour créer des maladies chez l'animal puis chez l'homme. Ce fut particulièrement le cas des Japonais lors de la seconde guerre mondiale.

Des agents pathogènes naturels nous posent déjà ces problèmes :

- le virus de la variole qui tue l'espèce humaine à 20 ou 40 % et qui est l'une des grandes menaces biologiques actuelles. Il est sanctuarisé aux États-Unis et en Russie ;
- le virus du sida qui tue à 95 % en l'absence de traitement ;
- le virus Ebola qui tue entre 50 et 90 % ;
- le virus du SARS qui a une mortalité de 6 %, ce qui est considérable ;
- le virus de la grippe espagnole qui avait une mortalité de 4 %, qui se transmet par aérosol et qui a tué près de 50 millions d'êtres humains en 1918 et 1919.

Ces agents pathogènes naturels sont bien connus. Ils sont une menace, les bio-terroristes peuvent les utiliser, mais on maîtrise à peu près l'avenir parce que l'on dispose des vaccins correspondants.

La biologie moléculaire est née dans les années 60. En générant un très grand nombre de données, elle a fait naître une nouvelle science très importante, la bio-informatique qui aura des conséquences dont je vous parlerai ultérieurement. Dans les années 85-90, les nanotechnologies ont apporté la miniaturisation et l'extrême sensibilité qui permet de détecter quelques molécules du vivant. Dans les années 60-70, on a donc pu cloner, c'est-à-dire explorer le vivant, isoler un gène et la protéine qu'il produit. On a pu amplifier des quantités infimes d'ADN par la technique de la PCR qui est extrêmement utilisée et qui a permis l'essor considérable des biotechnologies. On a commencé à séquencer des organismes entiers avec le séquençage d'une bactérie en 1995. En 2004, nous avons près de 200 génomes entièrement séquencés. 600 génomes sont en cours de séquençage, aussi bien le génome humain que celui d'animaux, de plantes, de bactéries, de virus. Tous les virus ont été séquencés et sont disponibles sur Internet. On peut faire des arbres phylogéniques, c'est-à-dire, en quelque sorte, des arbres généalogiques et l'on peut tracer très facilement l'identité d'une souche. Par exemple, on avait séquencé une souche de *Bacillus anthracis*, l'agent du charbon. 14 souches sont maintenant séquencées et disponibles.

On a commencé à manipuler le vivant en introduisant des gènes dans des êtres vivants pour les modifier. On peut remplacer un gène, le détruire, en ajouter un autre. C'est ce que l'on appelle la transgénèse, les OGM, et, dans la version « Docteur Jekyll », la thérapie génique. Mais je vais surtout vous parler aujourd'hui de « Mister Hyde », c'est-à-dire des utilisations de ces biotechnologies pour rendre un gène plus virulent ou plus dangereux. Depuis quelques années est apparue une nouvelle technologie appelée le *DNA shuffling* qui permet de créer des agents pathogènes complètement nouveaux. À mon avis, cela aura une importance dans les quinze ou vingt années à venir. On peut également synthétiser des gènes et même des agents pathogènes J'y reviendrai dans un instant.

Je parlerai tout d'abord des méthodes conventionnelles qui sont connues depuis quinze ans. On peut accroître la virulence ou la résistance d'un agent pathogène par l'introduction de gènes et rendre ainsi des bactéries plus résistantes à la dessiccation, aux ultraviolets, aux antibiotiques. Dans le programme Biopreparat, il a été indiqué qu'une souche d'Y*ersinia pestis*, l'agent de la peste, avait été rendue résistante à 16 antibiotiques. Ce n'est pas publié mais on peut éventuellement introduire des gènes extrêmement dangereux – par exemple, le gène de la toxine

botulinique – dans une souche inoffensive *d'Escherichia coli* qui est une bactérie de notre flore digestive. On peut également introduire des gènes qui stimulent la virulence. Une publication récente a montré qu'en introduisant le gène d'un facteur de croissance des lymphocytes (IL4), on rendait beaucoup plus virulente une souche de la variole de la souris appelée l'ectromélie.

Deux découvertes faites en 2002 et 2003 sont extrêmement inquiétantes. Pour la première fois, on a réussi à synthétiser le virus de la poliomyélite à partir de la séquence disponible sur les banques de données, totalement in vitro, indépendamment de toute culture. Le paradoxe est que l'on peut créer en laboratoire, par synthèse, en disposant simplement de la banque de données, ce virus qui sera éradiqué vers 2005 après une campagne d'éradication de l'OMS. Il a fallu trois ans pour aboutir à ce résultat. Aux États-Unis, Greg Venture a synthétisé un autre virus un peu plus petit en quinze jours. On peut donc maintenant synthétiser des virus, notamment celui de la variole qui est beaucoup plus difficile à réaliser. Ce type de technique désanctuarise certains virus inaccessibles - espérons-le - aux bio-terroristes. Greg Venture a indiqué dans la revue *Nature* qu'il était en train de fabriquer une bactérie totalement artificielle en regroupant 200 gènes. Ceci est extrêmement inquiétant pour Mister Hyde. La variole et n'importe quelle bactérie peuvent ainsi être créées.

La technique du *DNA shuffling* est apparue en 1994 aux États-Unis, «shuffling » signifiant « battre les cartes ». Elle a été sans cesse améliorée et fait l'objet de nombreuses publications aux États-Unis de la part de compagnies privées. Il s'agit de prendre un gène et deux ou trois autres gènes qui lui ressemblent, de le couper en petits morceaux – il est possible de le ré-assembler ensuite – et de générer ainsi des millions de mutants. Il est alors possible de sélectionner pour un caractère donné.
Sur plusieurs millions d'années, l'évolution permet d'obtenir, à partir d'un gène ancestral, un gène d'une première espèce, d'une seconde espèce, d'une troisième espèce, d'une quatrième espèce qui se différencient. Grâce à la technique du *DNA shuffling* il est désormais possible de réaliser cette mutation en quelques heures.

Je vais vous donner quelques exemples tout à fait inquiétants. En 2002, une expérience a été publiée dans la revue *Nature*. Elle a consisté à prendre six souches d'un rétrovirus responsable de leucémies de la souris et à les traiter par *DNA shuffling*. 5 millions de virus chimères ont ainsi été créés et ils ont ainsi pu obtenir, par sélection et en quelques heures, un virus capable d'infecter des cellules que la souche sauvage ne peut pas infecter. En d'autres termes, on peut changer le tropisme d'un virus. Imaginez quelles seraient les conséquences si l'on rendait le virus HIV transmissible par aérosol et permissif pour les cellules respiratoires.
La même équipe a réussi à rendre 32 000 fois plus résistante aux antibiotiques une souche *d'Escherichia coli* alors que par mutation avec les techniques classiques, il est difficile d'obtenir plus de 16 fois, ce qui est déjà beaucoup. Elle a ainsi pu produire une protéine du virus de la variole bloquant la réponse immunitaire.
Une technologie est apparue l'année dernière avec l'application du *DNA shuffling* aux souches bactériennes en faisant fusionner les bactéries entre elles, ce que l'on appelle la fusion protoplasme.
L'avenir est donc inquiétant parce que l'on peut synthétiser les agents infectieux à partir de leur séquence. De plus en plus de séquences sont publiées. Tous les virus

sont publiés et beaucoup de bactéries le sont également. On pourra ainsi reconstituer des agents infectieux tout à fait nouveaux et qui n'existent pas dans la nature.

En réponse à cela, je pourrais décliner – mais je n'ai pas le temps de le faire aujourd'hui – que l'on peut répondre avec les mêmes techniques en fabriquant des vaccins. C'est le côté « Docteur Jekyll ». Les nanotechnologies apporteront peut-être une réponse à ces organismes nouveaux qui pourraient se répandre à partir des biotechnologies. Des progrès incroyables ont été réalisés en imagerie moléculaire et pour les bio-senseurs. Le microscope à tunnel et le microscope à force atomique qui sont apparus dans les années 85-90 permettent de visualiser directement les atomes. Ce type de technologie permettra peut-être un jour de manipuler directement les atomes.

Dans les années 90-95, les biotechnologies avaient apporté les bio-puces qui ne sont pas des nanotechnologies mais qui consistent, par exemple, à explorer des milliers de gènes sur un minuscule morceau de plastique ou de verre. On peut ainsi étudier l'expression des gènes d'un génome entier - plusieurs dizaines de milliers de gènes - et également identifier rapidement des micro-organismes qui sont encore à l'état relativement expérimental.

Les nanotechnologies apportent la possibilité de faire des bio-senseurs d'une extrême sensibilité. Le principe est en apparence très simple. On les associe, à partir de nanostructures, de nanocâbles ou de nanoparticules, à des molécules biologiques, des liguants (molécules d'ADN, protéines, anticorps, enzymes, etc.). Lorsque le récepteur se lie à son liguant, un signal est généré parce qu'il y a un changement physique de la nanostructure. Ceci permet, en quelques secondes ou quelques minutes, de détecter des femtogrammes (10^{-12} mg), soit des quantités de l'ordre de quelques molécules.

Dans le bio-senseur, il y a un nanotube dans lequel on place un récepteur, par exemple un anticorps contre la toxine botulinique. Si cette dernière est détectée et qu'elle se lie à son anticorps spécifiquement, il y a une chute du courant électrique. On peut ensuite laver le biosenseur pour le régénérer. Je lisais dans un article de *Nature* que certaines compagnies fabriquent actuellement des nanolaboratoires, c'est-à-dire des microchips sur lesquels il y a des câbles contenant toute une série de senseurs contre de nombreuses protéines ou acides nucléiques. On pourrait ainsi, dans cinq ou dix ans, faire de multiples essais pour détecter très rapidement de nombreux agents infectieux ou pathogènes.

En conclusion, les biotechnologies et la bio-informatique sont actuellement à un tournant. On passe des armes biologiques classiques que l'on connaît depuis le début de l'humanité - le virus de la variole est connu depuis l'Antiquité - à des armes complètement nouvelles que personne ne connaît et ne connaîtra. On peut imaginer la fabrication d'un virus de la variole qui tue l'espèce humaine à 100 % ; un SARS extrêmement virulent aussi contagieux que le virus de la grippe ; un HIV qui se transmet par aérosol. Cela reste encore à un horizon de cinq à dix ans mais c'est possible. Il y a deux ou trois ans, je ne vous aurais pas tenu le même langage.

Ceci met en exergue l'importance du facteur temps. Puisque l'on ne pourra pas prévoir ce qui sera créé si des bio-terroristes utilisent ces technologies qui ne sont pas extrêmement compliquées, il s'agit de savoir combien de temps il faudra pour détecter cela et réagir. Les nanotechnologies, par les bio-senseurs, pourront identifier très précocement les agents infectieux. Les biotechnologies, se retournant contre les agresseurs utilisant le *DNA shuffling*, pourront créer des vaccins très rapidement ou éventuellement des antibiotiques pour résister à ces nouveaux agents infectieux.

(Applaudissements)

Jean-Louis GERGORIN
Merci Monsieur le Professeur pour cet exposé qui était à la fois fascinant et très inquiétant. Il se termine toutefois par une petite lueur puisque la combinaison des biotechnologies et des nanotechnologies peut être un facteur positif, notamment au niveau de la détection. C'est une excellente transition avec le sujet suivant qui porte sur les nanotechnologies et qui est présenté par le Professeur CAPPY.

Micro-systèmes et nanotechnologies

Alain CAPPY, directeur de l'Institut d'électronique, micro-systèmes, nanotechnologies de Lille
Je vais vous parler du passage entre les micro-technologies et les nanotechnologies. Il s'agit de savoir s'il s'agit d'une rupture ou d'une continuité. Nous vivons aujourd'hui l'ère des micro-technologies. Le terme de « micro-technologies » signifie que les dimensions typiques des objets manipulés sont le micromètre (un millionième de mètre). Par exemple, le diamètre d'un cheveu est de 50 à 100 microns. Cette ère des micro-technologies est constituée principalement par la micro-électronique, que vous connaissez très bien, mais également, depuis maintenant une quinzaine d'années, par d'autres technologies issues des technologies de la micro-électronique que sont les micro-systèmes avec des succès industriels incontestables tels que les accéléromètres (pour déclencher les airbags) et, en micro-fluidique, les têtes pour les imprimantes à jet d'encre. Aujourd'hui, nous vivons un passage de cette micro-électronique, dont la taille des objets est plutôt d'un micron, à des objets de taille nanométrique, c'est-à-dire d'un milliardième de nanomètre. Par exemple, un nanomètre représente dix atomes d'hydrogène mis côte à côte.

Il y a également une ouverture vers d'autres disciplines, ainsi que cela a été évoqué précédemment. Les nanotechnologies vont nous permettre de fabriquer des nanomatériaux. Il ne s'agit plus de se contenter des propriétés des matériaux qui sont à notre disposition dans la nature mais, au contraire, de fabriquer des matériaux aux propriétés particulières, c'est-à-dire en prédéterminant les propriétés et en fabriquant le matériau qui va avoir ces propriétés. Par exemple, de très nombreux travaux concernent aujourd'hui les nanocristaux avec des propriétés électriques, ferroélectriques, ferromagnétiques, optiques, mécaniques. Je parlerai un peu des nanotubes de carbone qui sont un exemple très intéressant de nanomatériaux.

Aujourd'hui, lorsque l'on fabrique un objet, on utilise la méthode dite descendante ou *top-down*. C'est-à-dire que l'on travaille un peu comme des sculpteurs en partant

d'un bloc énorme et en parvenant à fabriquer un petit objet par gravures successives. Une autre méthode commence à voir le jour, la méthode ascendante ou *bottom-up*. Elle concerne au contraire l'utilisation de molécules et d'atomes individuels que l'on va assembler pour former un objet de taille supérieure. Ce changement de mode de fabrication constituera très certainement une rupture très importante dans les années à venir.

Je vais maintenant vous présenter quelques exemples de micro-technologies et de nanotechnologies.

✓*Les micro-technologies*

Un microprocesseur comporte environ 30 à 40 millions de transistors. Un transistor est un objet dont la plus petite dimension est d'environ 100 nanomètres. L'exploit industriel est que ces 40 millions de composants fonctionnent tous, ce qui vous permet de regarder mon exposé grâce à l'ordinateur que j'utilise aujourd'hui. En ce qui concerne les micro-systèmes, les technologies issues de la micro-électronique ont permis la fabrication de bio-puces à ADN favorisant en particulier le séquençage du génome.

Un autre exemple est celui d'une micro-pince dont la distance entre les bras est d'environ 50 microns. Cette micro-pince est destinée à attraper des cellules. Elle est entièrement mécanique, c'est-à-dire que l'on a reconstitué des liaisons pivots permettant d'ouvrir et de fermer la pince.

Un troisième exemple de micro-technologie est celui de l'association entre le monde physique et le monde du vivant. On a fait se développer des neurones de rat sur des transistors. En excitant le transistor, on parvient à transmettre un signal électrique par l'intermédiaire des neurones puis à retrouver le signal transmis sur un autre transistor. C'est un domaine qui prendra de l'importance au fur et à mesure que l'on travaillera dans des dimensions de plus en plus petites et donc dans les dimensions des nanotechnologies.

La micro-électronique est un monde absolument merveilleux. Aujourd'hui, les microprocesseurs modernes contiennent une quarantaine de millions de transistors. En prolongeant cette évolution temporelle, on peut imaginer qu'ils comporteront un milliard de transistors en 2007. Si l'on intègre plus de dispositifs sur une surface qui reste à peu près constante, il faut évidemment que ces dispositifs soient de plus en plus petits, d'où le passage de « micro » à « nano ». Ces dispositifs sont également de plus en plus rapides. Entre 1970 et aujourd'hui, la fréquence de l'horloge des processeurs a été multipliée par dix tous les dix ans. On a donc gagné un facteur 1 000 en trente ans et les microprocesseurs travaillent aujourd'hui avec plusieurs giga-hertz. Cette évolution va se poursuivre dans les années futures.

Comment va se poursuivre cette évolution ? Les dimensions typiques des dispositifs étaient de 100 microns dans les années 60 et elles sont aujourd'hui de 100 nanomètres donc l'évolution est remarquable puisque c'est une décroissance exponentielle. On va donc prolonger cette loi afin d'aboutir à un modèle de développement que l'on se fixe pour le futur. C'est ce que l'on appelle la feuille de route de la micro-électronique. Les industriels travaillent pour suivre cette feuille de route. Jusqu'en 2010-2012, il ne devrait a priori pas y avoir d'accidents importants

sur cette feuille de route. En revanche, nous allons entrer dans des zones de turbulences à partir de cette date parce que la physique des dispositifs va changer. En effet, les dispositifs devenant de plus en plus petits, on va atteindre des dimensions où de nouveaux phénomènes vont apparaître. Entre les deux, les choses évolueront plus ou moins rapidement. On peut néanmoins penser que ce modèle de développement se réalisera dans les années 2020-2030 en atteignant des dimensions de quelques nanomètres. Aujourd'hui, aucune technologie capable de fabriquer ces dispositifs n'est envisagée.

Ce qui fait également la force de l'industrie micro-électronique, c'est le marché puisque, depuis les années 60, celui-ci croît de façon exponentielle, avec des hauts et des bas, et représente plusieurs centaines de milliards de dollars. Toutes ces prouesses technologiques n'existent évidemment que parce qu'il y a un marché. Les industriels n'investiraient pas des sommes colossales s'il n'y avait pas également un marché colossal.

✓*Les nanotechnologies*

On sait aujourd'hui parfaitement manipuler et observer des atomes et des molécules grâce à l'invention d'outils tels que les microscopes à champ proche. Il y a ensuite des conceptions et des fabrications de nouveaux matériaux. Il y a également de nombreux travaux sur les surfaces. Lorsque l'on diminue la taille d'un objet, on augmente toujours le rapport surface/volume. Plus les objets sont petits, plus les surfaces sont importantes. La nanostructuration des surfaces devient donc très importante. On peut par exemple imaginer de créer des nanopoils sur une surface pour la rendre insalissable ou lui donner d'autres propriétés.

Si l'on se projette à la fin ou au-delà de la feuille de route de la micro-électronique basée sur une approche semi-conducteurs, que peut-on imaginer comme dispositifs ? Dans le monde, de nombreux groupes travaillent sur l'électronique moléculaire. L'idée est de remplacer les dispositifs semi-conducteurs par des molécules qui auraient des propriétés identiques à celles des dispositifs de la micro-électronique.
Il est important de noter que dans le domaine dès nanotechnologies, on travaille nécessairement à l'interface entre les disciplines. Aujourd'hui, le physicien, le chimiste et le biologiste travaillent exactement dans le même domaine de dimension, avec les mêmes outils donc nécessairement ensemble. Par exemple, si l'on travaille sur une mémoire ou un calculateur à ADN, on ne fait ni de la physique, ni de la chimie, ni de la biologie mais le groupe qui travaille dans le domaine constitue un ensemble. C'est très important parce que l'enseignement est aujourd'hui essentiellement disciplinaire. Or il doit de plus en plus s'ouvrir aux disciplines annexes et surtout à l'interdisciplinarité.

On peut ainsi jeter des atomes de fer sur une surface en cuivre et les pousser un à un grâce au microscope à force atomique afin de créer un dessin. On peut faire mieux car il ne s'agit pas seulement de créer une image. On peut analyser la forme de la pointe et remonter à l'interaction entre l'atome et la surface.

✓*Les nanotubes*

Les nanotubes ont été découverts il y a une dizaine d'années. C'est une nouvelle forme du graphite utilisé dans les crayons. Le graphite est constitué de plans de

carbone qui se déposent sur le papier lorsque l'on écrit. On a constaté il y a peu de temps que l'on pouvait rouler ces feuilles de graphite pour former des tubes dont le diamètre est de quelques nanomètres. On forme ainsi une fibre dont les propriétés sont tout à fait extraordinaires. Selon la façon dont a été enroulée la feuille de graphite, on peut former des tubes conducteurs (totalement métalliques) ou semi-conducteurs (ayant des propriétés adaptées au traitement de l'information). On peut également utiliser ces tubes pour fabriquer des pointes qui émettent des électrons. On retrouve ce principe dans les écrans plats. Les propriétés mécaniques de ces nanotubes sont également tout à fait extraordinaires. Les nanotubes sont 100 fois plus résistants et 6 fois plus légers que l'acier.

Des nanotechnologies permettent donc aujourd'hui de créer des objets dont les propriétés sont encore relativement mal connues. Néanmoins un marché existe déjà et des sociétés fabriquent aujourd'hui des centaines de kilos de nanotubes par jour qui sont d'ailleurs essentiellement utilisés pour les matériaux composites.

✓L'électronique moléculaire

Le circuit d'un point mémoire d'ordinateur est normalement réalisé avec des transistors. On peut commencer à imaginer de refaire la même topologie, le même design avec des molécules. L'avantage du moléculaire est essentiellement la taille. La taille de la cellule mémoire sera de quelques nanomètres sur quelques nanomètres au lieu de 1 micron sur 1 micron, soit un gain de plusieurs ordres de grandeur en taille.

Il est très important de pouvoir développer la méthode ascendante dans le futur. En effet, on n'imagine pas de fabriquer un système d'électronique moléculaire en travaillant les molécules une à une. Il faut que le système s'auto-fabrique. Il y a aujourd'hui des exemples très intéressants. On a ainsi récemment démontré que l'on pouvait fabriquer des métallisations avec des bactéries. On a également utilisé le principe de l'ADN pour montrer que l'ADN ne peut pas se reproduire.

Je vais maintenant vous montrer un exemple de l'association de ces technologies, celui des poussières intelligentes. L'idée de Christopher Pister, de l'Université de Berkeley, a été de réaliser un ensemble de taille extrêmement petite (environ 1 mm^3) composé d'un capteur, d'un récepteur, d'un émetteur, d'un système électronique qui permettra de gérer l'ensemble et d'un système de batteries qui générera l'énergie nécessaire. Il s'agit ensuite de disposer ces poussières intelligentes dans un terrain. Elles se mettent automatiquement en réseau, font les mesures nécessaires et, en s'interconnectant, transmettent une information par l'intermédiaire d'une antenne ou par un autre biais. Cela forme donc un réseau *ad hoc* constitué de millions de poussières. Lorsque deux poussières veulent communiquer, elles passent par un chemin. En fait, il n'y a pas de centralisation mais toute l'information passe par les différentes poussières.

En conclusion, on dispose d'une feuille de route assez claire pour la micro-électronique et la nanoélectronique jusqu'en 2018. Les choses sont ensuite beaucoup moins limpides. Il n'existe actuellement aucune technologie identifiée pour l'ère post-feuille de route.
Le point important est que les nanotechnologies concernent une convergence entre différentes disciplines ; qu'il y a des ruptures possibles dans les procédés de

fabrication ; qu'il ne faut pas penser que les innovations ne proviennent que des matériaux et des dispositifs parce qu'elles proviennent également des associations de technologies. Je suis persuadé que les vraies ruptures se produiront lorsque l'on parviendra à associer de façon intelligente semi-conducteurs, molécules, ADN, nanotubes et autres. Je vous remercie.

(Applaudissements)

Jean-Louis GERGORIN
Merci Monsieur le Professeur. Nous allons passer de la micro-électronique au traitement de l'information qui est évidemment au cœur de la révolution de la guerre en réseau dont nous avons parlé ce matin. Je passe la parole à l'ingénieur général FAYARD, directeur du SPOTI à la DGA.

Systèmes d'information

François FAYARD, directeur du SPOTI, DGA
Mon propos est à rapporter à celui de l'amiral TANDONNET qui a fait un exposé prospectif sur les nouvelles technologies. En ce qui me concerne, je vais parler de la façon dont nous implémentons ces nouvelles technologies dans les programmes des années à venir et expliquer comment cela pourrait changer la façon de travailler de nos armées et améliorer leur efficacité.

Le système de communication et d'information a la forme classique d'un système d'armes :

- observer davantage ;
- transmettre plus rapidement ;
- décider sûrement.

En ce qui concerne le spatial, 2004 est une année forte pour nous puisque nous allons lancer Hélios à la fin de l'année. C'est un satellite de 5 tonnes qui transmettra des images optiques classifiées mais aussi belles et indiscrètes que les images prises depuis un hélicoptère à 300 pieds du sol. Elles permettent de tout voir jusqu'au détail le plus fin. Hélios permettra aussi de voir de nuit. Ce qui est également très nouveau, c'est que non seulement on enverra l'imagerie d'Hélios à la DRM et au pouvoir politique mais on l'enverra également dans quinze sites de France délocalisés (Brest, Toulon ou ailleurs) très peu de temps après la demande.

Nos alliés italiens et allemands ont lancé l'imagerie spatiale radar (Sar-Lupe pour l'Allemagne et Cosmos-Skymed pour l'Italie). À partir de 2007, nous recevrons des centaines d'images radars tous les jours, ce qui sera passionnant, non interprété et qui ne manquera pas de saturer nos réseaux. On fait du NCW mais cela pose des problèmes de réseaux lorsqu'il faut transmettre des images radars à tout le monde.

Le troisième aspect des choses, moins connu, est la géographie numérique. Il n'y a plus de système d'armes sans géographie, sans localisation précise, sans *targeting* précis. C'est le spatial - essentiellement Spot 5 - qui permettra d'obtenir dans les années à venir une cartographie de n'importe quel point du globe - même là où il n'y

a pas de cartes disponibles - avec une très grande résolution. La défense française et le Pentagone sont les deux meilleurs clients de Spot Images.

Nous allons donc passer à un renseignement extrêmement abondant en termes de nombre d'images, spatiales en particulier. Il faudra non seulement que les photo-interprètes les analysent mais qu'elles soient diffusées à tout le monde. C'est un enjeu magnifique pour les cinq années qui viennent.

La génération future des satellites misera avant tout sur l'écoute des liaisons radios ou des radars. Le satellite S1 est gros comme une machine à laver. Je pense qu'avec 3 ou 4 satellites S1, on pourra remplacer le DC8 Sarigue, le MINREM. J'exagère un peu mais on aura la capacité d'accéder à n'importe quel signal radio-électrique au-dessus de la terre en tout lieu et en tout temps avec une fréquence qui dépendra de la rotation de S1. C'est assez fantastique.

Les missiles longue portée sol-sol sont une vraie menace pour nos forces. Avec le démonstrateur Alerte que nous allons lancer dans l'espace en 2006-2007, on pourra détecter tous les missiles longue portée, l'endroit d'où ils viennent et, si possible, identifier l'agresseur.
Un autre démonstrateur spatial, LOLA (liaison optique laser), apportera la preuve que l'on pourra transmettre, à partir de 2010, des images à très haut débit par liaison laser (par exemple depuis un drone qui prendra les images, via un satellite relais géostationnaire jusqu'à une station sol).

Un autre aspect des choses est d'offrir un service de bout en bout. Nos armées interviennent de plus en plus partout et le rêve de tous les militaires est de disposer sur un théâtre d'opérations du même service de type Internet qu'ils ont à la maison ou au bureau. C'est facile à dire, c'est plus compliqué à réaliser. Ce qui nous sauve aujourd'hui, c'est la technologie IP. Nous disposons aujourd'hui d'un certain nombre de réseaux (le réseau de transit Socrate, les réseaux des bases aériennes, les réseaux de la Marine, les réseaux de l'Armée de terre, les réseaux HF pour l'outremer, les réseaux alliés). Tous ces réseaux sont évidemment en métropole. Début 2005 sera lancé Syracuse 3 qui permettra, sur tous les théâtres d'opérations qu'il couvrira (Afrique, Asie, Europe), d'avoir le même service IP qu'à la maison. On saura également « boucher les trous » entre les différents réseaux de transit et les réseaux de desserte. C'est donc un programme considérable qui débouchera, pour l'essentiel, en 2006, 2007 et 2008.

Comment mettre en œuvre ces réseaux IP ? À l'origine, il y a des réseaux IP d'armée (terre, air, mer) et les réseaux opératifs puisque les opérations sont en général inter-armées. La différence essentielle entre un opérateur civil et les opérateurs militaires est que ces derniers sont plusieurs en France et qu'ils ont surtout le défaut de bouger. Or ils estiment avoir le droit de pouvoir accéder aux services partout où ils se trouvent dans le monde. Ils se trouvent de plus dans des lieux, notamment en opérations, où il n'y a pas beaucoup de débit et d'infrastructures. Les réseaux IP sont donc peu homogènes. Il y a en particulier une partie bas débit, la partie radio.

Dans la défense, on a fait la promotion d'une architecture IP appelée Attila qui a non seulement pour but de connecter des réseaux IP entre eux mais également d'être

capable d'oublier que les réseaux physiques sont aujourd'hui un peu disjoints entre eux. Elle crée une espèce de sur-couche afin de pouvoir apporter tous les services Internet à n'importe quel abonné présent sur un des réseaux et déclaré. Attila permet donc d'avoir un service ISP (*Internet Service Provider*) en théâtre d'opérations identique à celui dont on dispose à la maison, quelle que soit l'armée d'origine à laquelle on appartient. Cela vous paraît évident mais ce n'est pas si facile lorsque l'on sait que tous ces réseaux ont été développés de façon séparée. Attila permet également de superviser les services communs à tous ces réseaux, en particulier les annuaires, les DMZ (zones de protection), les socles communs, etc. Il permet de prendre en compte les bascules, c'est-à-dire de suivre la trace des personnes qui se déplacent dès qu'elles se déclarent à nouveau. Il y aura l'outil physique, il n'y aura plus qu'à mettre en œuvre l'organisation pour que les réseaux IP des armées soient parfaitement homogènes. Cette architecture Attila a été adoptée par la totalité de la défense début 2003. Elle est implémentée par la Marine et les autres armées suivent. On peut espérer avoir un réseau IP souple dans les armées à partir de 2007.

La partie système d'information, applicatifs métiers, est un peu plus compliquée. Il y a actuellement 21 programmes d'armement différents. C'est un puzzle parce que chaque armée a lancé ses propres programmes, ce qui était naturel et nécessaire puisque c'était compliqué au départ. Il faut maintenant atteindre une cohérence - du niveau tactique au niveau politique - avec les alliés et entre les armées (notion qui n'existait pas encore il y a cinq ou six ans). Comment s'y prendre ? Ce n'est pas facile puisqu'il n'y a pas de protocole IP au niveau des applicatifs métiers. On ne sait d'ailleurs pas très bien ce que l'on veut échanger entre armées ou avec les alliés.
Je voudrais évoquer l'effort réalisé par l'Armée de terre pour numériser l'espace de bataille. Un travail considérable a été effectué pour développer des SIC (systèmes d'information) bâtis sur un socle commun qui assurent tous les services communs et sur lesquels viennent simplement se greffer les applicatifs métiers. À partir de 2008-2009, les armées disposeront de systèmes d'informations parfaitement interopérables grâce à ce socle commun, chaque armée venant ajouter son applicatif métiers.

L'aspect sécurité se divise en deux. Le renseignement et les écoutes sont l'art de la guerre. Les armées ne sont pas très fortes dans le domaine des écoutes. Les moyens sont un peu vieillissants. Or les écoutes permettent les interceptions de satellites, de faisceaux hertziens, de branchements parasites, de GSM, de mises en place de virus d'attaque dans les ordinateurs, de chevaux de Troie, de portes dérobées, etc. C'est facile à faire et il faut le faire lorsque l'on veut attaquer. Méfiez-vous et protégez-vous parce que l'on peut également écouter les téléphones.
Les armées se préoccupent de cela et vont développer des intranets sécurisés dans lesquels l'on pourra s'authentifier et chiffrer ses messages. Cela progresse lentement. On a beaucoup parlé des attaques potentielles, que l'on connaît, mais, comme pour les virus, il me semble que l'on est plus fort pour les attaques que pour la défense. La protection existe, il faut s'en occuper.

Les systèmes d'information et de commandement sont devenus un véritable système d'armes. On est passé de la simple bureautique qui rend un grand service à un système d'armes. Mon credo est que dans les années qui viennent, cette chaîne « observation-transmission-renseignement-décision » sera infiniment plus performante qu'aujourd'hui puisque tous les grands programmes - depuis Hélios 2

jusqu'au système de commandement qui servira pour l'îlot Saint-Germain - arriveront en même temps entre 2006 et 2008. J'espère que les armées en seront satisfaites.

(Applaudissements)

Jean-Louis GERGORIN
Merci Monsieur l'Ingénieur général pour cet exposé très dense qui est un remarquable succès en termes d'algorithmes de compression de données parce que nous avons beaucoup appris en peu de temps.

Je passe maintenant la parole à notre dernier orateur, Monsieur Claude GUET qui est directeur scientifique de la Direction des applications militaires du CEA. Il va intervenir sur les technologies dont on a beaucoup parlé il y a quinze ans et dont on reparle à nouveau énormément et qui concernent l'énergie dirigée. Celle-ci est importante pour maintenir le niveau de notre force de dissuasion et dans d'autres applications plus offensives dont nous pourrons reparler.

Energie dirigée

Claude GUET, directeur scientifique CEA/DAM

Le concept d'armes à énergie dirigée (AED) date de 1983 lorsque le Président Reagan annonçait son initiative de défense stratégique en donnant pour objectif d'intercepter et de détruire des missiles balistiques avant qu'ils n'atteignent le sol américain. La bonne solution est une impulsion électromagnétique parce que, d'une part, elle peut être dirigée précisément sur de longues distances et, d'autre part, la propagation est quasiment instantanée. Il apparaît aujourd'hui que l'on peut classer les AED en trois grandes catégories :

- les lasers de haute énergie, thème qui aurait été abordé par Monsieur BATTISTELLA :
- les lasers de haute puissance ;
- les micro-ondes de forte puissance (MFP) qui fournissent des impulsions radiofréquence.

Il y a enfin les faisceaux de particules chargées. Cela n'a pas été très développé mais je souhaiterais en parler dans le contexte laser. Je m'étendrai sur les lasers de haute puissance et dirai quelques mots sur les lasers de haute énergie. Ces armes à énergie dirigée peuvent évidemment avoir des applications beaucoup plus larges que celles qui avaient été envisagées initialement et nous y reviendrons.

✓Les micro-ondes de forte puissance
L'objectif est de produire des bouffées intenses d'énergie électromagnétique sur la gamme de fréquences qui s'étendent typiquement de la centaine de mégahertz à plusieurs dizaines de gigahertz. Le principe d'une arme MFP est d'avoir une alimentation qui soit un générateur électrique puissant. Il peut également s'agir d'une explosion couplée avec un système électromagnétique ou éventuellement - ce n'est alors plus de l'énergie dirigée - une explosion nucléaire. Après couplage à une source micro-ondes et à une antenne, il s'agit de produire ce *pulse*

électromagnétique intense dont l'objectif est d'endommager les circuits électroniques de façon temporaire ou permanente ou de les détruire complètement. Tout cela dépend évidemment de la quantité d'énergie emportée par le *pulse* et du couplage de ce *pulse* à la cible.

Pour le physicien, il s'agit de comprendre et de trouver les solutions par un bon couplage des ondes hyperfréquences à la cible. De façon très schématique, nous avons deux possibilités :

- une pénétration par les ouvertures et les fentes
  Le système répond alors sur une très large bande mais il y a de nombreuses fréquences de résonance qui sont en général bien identifiées. Les énergies à apporter sont de l'ordre du watt au kilowatt par centimètre carré.

- un couplage direct aux fréquences de fonctionnement du système, soit une pénétration par la voie d'émission ou de réception du système.

Ce qui va caractériser les différentes armes MFP, ce sera la forme des ondes de haute fréquence. On parle de systèmes à bandes étroites dans le cas où l'on veut agir au niveau d'une fréquence de résonance bien identifiée. Il peut s'agir d'un seul coup qui porte une très grande puissance (par exemple, l'arme flash avec des puissances crêtes de l'ordre du gigawatt et des durées d'impulsion de quelques centaines de nanosecondes). Cela peut également être une salve d'impulsions de fréquences différentes. Il faudra alors coupler plusieurs sources de puissance élevée. L'autre approche consiste à couvrir par une bande large. Les puissances crêtes sont évidemment beaucoup plus faibles.

Un exemple de concept mono-coup bande étroite avec un Vircator est celui de l'arme flash. Le spectre hyperfréquence est produit par l'oscillation des électrons entre la cathode et une cathode virtuelle qui est due à la charge d'espace. L'analyse spectrale montre que sur une durée d'environ 200 nanosecondes, la fréquence, de l'ordre de 2.5 gigahertz, est à peu près constante.

✓*Les lasers à impulsion ultra courte*

L'objectif d'un laser haute puissance à impulsion ultra courte est d'avoir une puissance qui se situe au-dessus d'un seuil de puissance qui correspond à l'auto-focalisation non linéaire du faisceau. Pour une énergie donnée, on peut donc augmenter la puissance en diminuant la durée du *pulse*. Les *pulse* lasers dont je parle maintenant ont des durées qui sont inférieures à quelques centaines de femtosecondes (10^{-15} secondes) avec des énergies de l'ordre du joule à la dizaine de joules.

- **la propagation dans l'atmosphère sous forme de filamentation et de lumière blanche**

Que se passe-t-il lorsque l'on propage un faisceau laser dans l'air dans ces conditions ? L'indice de l'air - qui dépend de l'intensité - et le profil de densité transverse du laser vont conduire à une focalisation sur le centre de l'impulsion. C'est

ce que l'on appelle l'effet Kerr qui conduit donc à une auto-focalisation. L'intensité au centre devenant très grande, une ionisation multiphotonique va se produire et conduire à un plasma qui aura un effet de dé-focalisation. Il y a donc un autoguidage du faisceau laser sous la forme, par exemple, de bouquets de filaments avec une propagation sur plusieurs kilomètres.

Le projet Teramobile est une expérience réalisée dans le cadre d'une coopération entre deux laboratoires du CNRS et deux laboratoires allemands. Le laser est porté sur un camion. C'est un laser dont l'énergie dans le *pulse* est de l'ordre de 300 à 400 millijoules. La durée d'impulsion est de 70 femtosecondes, ce qui correspond à une puissance crête de 5 terrawatts pour une longueur d'onde de 800 nanomètres. Le faisceau a été tiré du toit de l'Hôpital de la Charité à Berlin et on a observé un canal de lumière blanche qui s'étendait sur une vingtaine de kilomètres. La puissance de ce laser est d'environ 700 fois la puissance seuil.

Quelles peuvent être les applications défense de ces lasers haute puissance ? Une première application est une extension du LIDAR (*LIght Detection And Ranging*). L'avantage est de pouvoir faire une propagation sur de très longues distances et d'avoir une lumière blanche donc un très large spectre. On peut donc faire une analyse spectroscopique sur une très large bande. On retrouve les applications habituelles de télémétrie et d'imagerie. C'est un moyen beaucoup plus efficace pour l'analyse, par exemple, d'aérosols et de détection d'agents bactériologiques. Pour ce type d'application, les énergies lasers nécessaires restent inférieures à la dizaine de joules. Pour des énergies supérieures à la dizaine de joules, on peut envisager des applications de brouillage et d'endommagement.

- **la production de faisceaux d'électrons de haute-énergie**

Un laser très intense suppose un champ électrique très supérieur à celui qui est à l'intérieur de l'atome. Le gaz que ce laser va irradier est complètement ionisé. Un plasma totalement ionisé peut supporter des champs intenses et des accélérations extrêmes de l'ordre du terravolt par mètre. Cela signifie que l'on peut, sur des distances millimétriques, obtenir des gains d'énergie gigantesques. Dans un gaz irradié par un *pulse* laser, on sait aujourd'hui qu'il y a l'action combinée de trois phénomènes physiques :

- la force pondéromotrice qui est proportionnelle au gradient de l'intensité du laser ;

- l'auto-focalisation relativiste
  L'indice de réfraction dépend de la masse de l'électron. Il y a une correction relativiste sur cette masse :

- l'onde plasma créée va en s'amplifiant et atteint un régime de rupture conduisant à la libération d'une bouffée d'électrons. Il a ainsi été démontré en laboratoire que l'on pouvait créer des paquets d'électrons relativistes.

Je citerai l'exemple obtenu récemment par le laboratoire d'optique appliquée. Un laser d'un joule, d'une largeur de 30 femtosecondes irradie un gaz. On observe alors deux ensembles de points dépendant de la densité du plasma et des électrons allant

jusqu'à 200 MeV avec une énergie moyenne des électrons de 18 MeV et une charge totale de 5 nanocoulombs.

Ainsi que cela a été dit précédemment pour la micro-électronique, les performances lasers croissent extrêmement rapidement. On peut envisager prochainement des lasers à 10^{20} watts/cm² avec des durées de *pulse* de l'ordre de la dizaine de femtosecondes. Le calcul montre que l'on peut probablement obtenir des bouffées contenant plus de 10 électrons d'énergies supérieures à un MeV, soit une énergie totale de la bouffée de 140 000 joules. Cela signifie une efficacité de conversion de l'énergie laser en énergie d'électron qui est de 22 %. On pourra également augmenter de façon tout à fait sensible la fréquence de répétition pour atteindre le kilohertz.
Des extensions immédiates ont déjà été démontrées en laboratoire. En faisant inter-réagir ce faisceau d'électrons avec le faisceau laser, on peut produire une source X intense. En faisant inter-réagir les électrons avec un élément de charge élevée, on peut produire une source de rayonnement gamma. Ceci a été observé sous forme de photofission de l'uranium. On peut donc induire la photofission de l'uranium à partir d'une interaction laser.

✓Les perspectives
Les performances des lasers ultra courts sont en très forte croissance. Doit-on s'attendre à des surprises ? Cette question a déjà été débattue. La difficulté est que, dans le domaine des innovations, les prédictions deviennent extrêmement difficiles. Je pense que l'on est loin d'avoir couvert toutes les possibilités qu'offrent les lasers de haute puissance.
En ce qui concerne les micro-ondes de forte puissance, la physique est mieux connue. Des développements technologiques importants doivent toutefois être poursuivis.

En conclusion, je pense qu'il y a un besoin constant d'études amont dans tous ces domaines.

(Applaudissements)

Jean-Louis GERGORIN
Merci infiniment. Je souhaiterais résumer très brièvement quelques leçons de ces exposés absolument passionnants.

Nous avons pu constater, en écoutant les différents orateurs, à quel point la communauté scientifique française se situe au niveau le plus pointu dans les grands domaines innovants qui ont été mentionnés. Nous n'avons aucun complexe à avoir.

Comme l'a souligné l'amiral TANDONNET, les armées ont un besoin très fort de pouvoir bénéficier de façon pratique des innovations technologiques.

Cela n'a pas été dit mais nous le savons tous : contrairement à ce qui se passe dans d'autres pays, notamment aux États-Unis, il existe un trop grand fossé entre la communauté scientifique et la communauté de défense. Nous connaissons bien sûr tous des contre-exemples. Les industriels de la défense qui sont représentés ici se situent d'ailleurs au plus haut niveau européen, sinon mondial, en termes de

dépenses consacrées à la recherche. En dépit de cela, nous n'avons pas l'équivalent de la DARPA en France et en Europe. Je rappelle que la DARPA dispose d'un budget de 2 milliards de dollars annuels. C'est beaucoup en termes de recherche mais relativement peu par rapport aux 400 milliards de dollars du budget américain de la défense. La DARPA finance beaucoup d'activités duales ou même civiles mais dont les retombées en termes de recherche avancée peuvent avoir un impact sur la défense. Elle a d'ailleurs été à l'origine d'innovations telles que l'Arpanet qui a donné Internet, le microprocesseur et toutes sortes d'autres grandes innovations.

J'élargirai la demande de Monsieur GUET. Nous n'avons pas seulement besoin de plus de recherches amont, nous avons besoin d'un changement d'état d'esprit, de créer une véritable communauté scientifique de défense, de rapprocher les chercheurs, les industriels et les responsables de notre défense dans une même démarche. Je pense que c'est un objectif qui peut être réalisé au niveau national. La réforme de la Délégation générale à l'armement qui est actuellement en cours en sera peut-être un instrument. Nous pouvons en tout cas l'espérer. Nous pouvons également espérer que l'Agence européenne de défense ne sera pas simplement un instrument pour diplomates mais un instrument effectif de définition de besoins et de définition de capacités de programmes technologiques et d'armements avancés.

Nous allons maintenant pouvoir débattre. Je vais abuser une dernière fois de mon rôle de président en posant deux questions liées à l'un des intervenants qui mérite d'être sélectionné parce qu'il a posé des questions qui mettent en cause notre survie à tous. C'est le Professeur BERCHE. Il nous a présenté des perspectives terrifiantes sur les possibilités des armes biologiques.

Ma première question est la suivante : quel est actuellement l'état de circulation et de développement dans le monde de ces moyens de mort que vous nous avez décrits ? Tout le monde dispose officiellement d'armes biologiques offensives et nous savons que de tels développements se produisent. D'autre part, quel est le risque, à partir de l'immense programme soviétique Biopreparat largement révélé par différents ouvrages et articles, que différents groupes (terroristes, mafieux ou autres) se soient procuré des souches ou divers produits développés dans cet immense complexe qui a employé des dizaines de milliers de scientifiques dans l'ex-Union soviétique ?

Ma seconde question est à la fois philosophique et pratique : n'y a-t-il pas une contradiction entre le besoin de sécurité et le principe de liberté de circulation de l'information scientifique ? N'est-il pas terrifiant que l'on puisse trouver sur Internet ou en lisant *Nature* ou *Science* le mode d'emploi pour créer tel ou tel virus ou bactérie particulièrement mortels ?

Patrick BERCHE
On pense qu'une dizaine de pays détient des armes biologiques extrêmement dangereuses, notamment, pour certains d'entre eux, le virus de la variole qui semble être l'un des plus dangereux actuellement puisqu'il est transmissible par aérosol. Des simulations indiquent que des centaines de milliers de personnes pourraient être atteintes en cas d'attaque. Je ne suis pas d'accord avec ce type de simulations probablement exagérées. Il existe certainement un certain nombre de pays « voyous » ou de groupes terroristes qui peuvent avoir accès à des virus dangereux tels que le virus Ebola. Je ne citerai que l'exemple de la secte Aum qui, en 1995,

avait fait une attaque au gaz sarin dans le métro de Tokyo. À plusieurs reprises, elle avait essayé, sans succès, de faire des attaques dans le métro avec le virus Ebola.

Personne n'est certain de ce qui va arriver avec les armes biologiques. Il faut savoir que toutes les publications portant sur les nouvelles technologies que j'ai décrites et qui peuvent conduire à des armes nouvelles sont disponibles. C'est effrayant. Certains scientifiques disent qu'il faut garder la liberté totale de publier les résultats. En ce qui concerne le virus de la variole de la souris, l'ectromélie, dans lequel on a ajouté un gène par hasard – il s'agissait de créer un virus pour tout à fait autre chose et l'on a constaté qu'il tuait les souris, mêmes vaccinées, à 100 % –, le papier a été retenu pendant plusieurs mois avant d'être publié. Il y a actuellement un débat dans la communauté scientifique. Faut-il publier les séquences des virus les plus dangereux ? Le virus de la variole est malheureusement disponible depuis 1992 et tout le monde dispose des séquences. C'est une question qui n'est pas encore tranchée.

Je pense que c'est dans ces armes qu'il y a de plus de dangers. Nous avons des réponses pour les armes classiques. On pourra contenir une attaque par la variole ou par le charbon. L'effet psychologique sera terrible mais le nombre des victimes sera probablement limité. En revanche, en cas de nouveau virus, par exemple un SARS extrêmement virulent - ce qui est tout à fait possible avec les technologies relativement simples que je vous ai expliquées -, personne ne maîtrisera la situation.

Jean-Louis GERGORIN
Merci Monsieur le Professeur. Je remarquerai simplement pour notre réflexion que nous estimons tous légitime qu'un certain nombre d'informations, par exemple sur la fusion thermonucléaire, soient protégées par des niveaux très élevés de classification dans nos pays alors que ces armes biologiques terrifiantes ne font l'objet d'aucune protection et d'aucune réglementation au niveau de la circulation de l'information.

Professeur BERCHE
Il y en aura probablement dans les années qui viennent.

Jean-Louis GERGORIN
Cela me paraît tout à fait prévisible. La parole est à la salle.

Amiral DURTESTE, Fondation pour la recherche stratégique
Monsieur GUET nous a parlé d'énergie émise sur les armes à énergie dirigée mais ce qui intéresse le militaire, ce n'est pas que vous soyez capable de sortir un gigawatt pendant quelques femtosecondes mais que vous puissiez répondre à la triple question : quelle létalité ? sur quelle cible ? à quelle distance ? Pouvez-vous me donner des indications ?

Claude GUET
J'ai fait le choix de présenter, ainsi que cela m'était demandé, l'état des recherches amont et les possibilités qui sont ouvertes dans le domaine des lasers haute intensité et impulsion courte. Je pense que c'est un autre débat que de discuter des effets directs de ces armes en termes de létalité. J'ai toutefois donné des exemples. Ce qui m'a semblé important, et qui est peut-être l'un des points les plus prometteurs dans

le domaine des lasers à impulsion courte, c'est l'extension des techniques LIDAR, notamment sur un très large domaine de fréquences. On émet en fait de la lumière sur une fréquence qui va de l'ultraviolet à l'infrarouge. Je n'ai peut-être pas suffisamment insisté sur ce point. Quand l'émission est extrêmement bien focalisée, on a une diffusion aux angles arrières. Cela permet de réaliser une analyse des composants chimiques ou biologiques à l'intérieur d'un aérosol avec une sonde très large bande. J'ai mentionné d'autres applications telles que les brouillages ou l'endommagement, par exemple de matériaux optiques.

Intervenant dans la salle
Nous savons que les technologies actuelles ont été créées pour les conflits classiques. De nouveaux conflits naissent aujourd'hui avec de nouvelles menaces et des modes d'action différents. Je m'adresse à l'ingénieur général : ces nouvelles technologies prennent-elles en compte ces nouveaux modes d'action ou vont-elles dans ce sens ? Notamment dans le domaine de la maîtrise du renseignement, cela permettrait une meilleure planification, une meilleure décision. Venant de l'Afrique centrale et étant voisin des Grands lacs, je suis très intéressé par ces technologies assimilables à des outils de veille préventive.

Jean TANDONNET
Notre difficulté est de savoir quelles sont les technologies prometteuses qui pourront dans l'avenir déboucher sur des systèmes d'armes. C'est un problème qui n'est déjà pas simple pour des conflits classiques. Dès que l'on s'intéresse à des problèmes de conflits asymétriques, la question devient beaucoup plus difficile. C'est tout le débat qui a été soulevé sur les armes biologiques, etc. Il est très difficile de savoir s'il n'y aura pas encore autre chose dans les dix ou quinze ans à venir dans ce type de conflits qui amèneront des armes contre lesquelles il sera difficile de se prémunir.

Monsieur FAYES, groupe BARCO
Les exposés concernant les nanotechnologies, l'informatique et la biologie étaient très intéressants. Aux États-Unis, des groupes de travail sont fortement constitués sur le NBIC, le C signifiant « cognitif ». On voit bien que le C nous conduits à l'art de la guerre, c'est-à-dire que toutes ces technologies vont provoquer des ruptures. C'est une puissance pour pouvoir mener la guerre mais on doit faire attention à l'aspect cognitif, au facteur humain, celui qui va rassembler l'information, prendre la décision et être efficace. Je souhaiterais savoir si, dans vos domaines respectifs, vous avez conscience des travaux qui sont menés aux États-Unis dans le domaine du NBIC. Comment la France compte-t-elle se positionner par rapport à ces recherches qui sont la finalité de la sélection et de l'utilisation de ces technologies ?

Jean TANDONNET
Dans la dernière partie de mon exposé, je n'ai pu m'empêcher de parler de l'homme et je vous rejoins tout à fait. Tous ces systèmes d'armes doivent être servis par des hommes et le facteur humain est extrêmement important. À travers ce que l'on a pu voir en Irak, il est évident que l'impact que l'on peut avoir par exemple sur le stress des personnes qui ont à se servir d'armes est capital. Il y a certainement un travail à réaliser dans ce domaine et je pense qu'il peut avoir un impact important sur nos doctrines. Le centre de doctrines interarmées qui verra le jour l'été prochain s'intéressera à ces problèmes de manière beaucoup plus fondamentale. Vous avez

raison, il faut également s'intéresser à tous les travaux menés en amont qui peuvent avoir un intérêt dans ce domaine.

Jean-Louis GERGORIN
Merci Amiral. Une dernière question.

Ingénieur général DE SAINT-GERMAIN
En écoutant l'exposé de l'amiral TANDONNET, j'ai été frappé qu'il ait surtout parlé des technologies innovantes dans le domaine de l'offensive alors que Monsieur BERCHE et l'ingénieur général FAYARD ont un peu mis l'accent sur des risques venant de l'extérieur vis-à-vis desquels il faut se défendre. Monsieur FAYARD a fait allusion aux virus, aux chevaux de Troie et à d'autres éléments du même genre qui peuvent infester complètement les merveilleux sites que nous aurons. N'y a-t-il pas également une recherche à effectuer en matière de technologies défensives, contre de nouveaux risques qui ne sont pas encore identifiés mais qui seraient très importants pour l'avenir ? Est-ce pris en compte par les OCO ?

Jean TANDONNET
La protection est importante et j'en ai parlé à travers les matériaux. Dans les innovations et les avancées importantes des prochaines années, je pense qu'il y aura le domaine essentiel de la protection avec les nouveaux matériaux que j'ai pu évoquer brièvement.

François FAYARD
Le problème est que plus on transmet, plus on informe, plus on prend le risque que son information soit attaquée. C'est malheureusement inévitable. Cela n'a pas empêché de travailler mais je pense qu'il faudrait vraiment développer des moyens défensifs tels que des moyens de chiffrement ou de signature électronique parce que nous sommes un peu en retard. Je rejoins ce que vous disiez. On pense effectivement plus à la domination par l'information et moins à se protéger.

Jean-Louis GERGORIN
Merci. La question de l'ingénieur général de Saint-Germain nous permet de tirer la conclusion d'ensemble de ce débat passionnant : la communauté de la science et de la technologie et la communauté de défense ont besoin l'une de l'autre. Comme l'amiral TANDONNET l'a souligné, la communauté de défense a besoin de l'apport de la science et de la technologie au niveau de la perception de la menace et des moyens d'y répondre. La communauté scientifique, quant à elle, ne peut plus rester dans sa tour d'ivoire. Même si elle est en général d'humeur peu guerrière, elle a un devoir de survie et de protection et ne peut pas se désintéresser de la nécessité de protéger la communauté humaine contre les nouvelles menaces qui ont été mentionnées. Ces deux communautés devront donc travailler ensemble en France comme elles le font ailleurs.

(Applaudissements)