PARLEMENT EUROPÉEN
« SOUS-COMMISSION SÉCURITÉ ET DÉFENSE »
AUDIT
19 JUIN 2013

Général (2S) Eric DELL'ARIA

« Pour faire suite à ces premières considérations conceptuelles, nous avons souhaité évoquer l'aspect pratique du dossier en gardant en tête la dimension opérationnelle d'une relance de la PSDC. Dans le contexte de crise internationale quasi-permanent auquel l'Union européenne est confronté, et face auquel la volonté politique doit pouvoir s'appuyer sur un ensemble d'outils efficaces et financièrement soutenables, seront traités ainsi deux secteurs sensibles que sont : le renseignement et le cyberespace, complétés de quelques autres suggestions susceptibles d'intéresser les travaux préparatoires au Conseil de décembre.

Le renseignement tout d'abord.

Le succès de toute politique extérieure est conditionné par le recueil puis l'exploitation d'informations fiables. Les théâtres récents sur lesquels l'Union européenne est intervenue ont rappelé la prépondérance du Renseignement, qui requiert des équipements toujours plus sophistiqués, des personnels toujours mieux formés, une interopérabilité obligée et une vérification constante des sources.
Le Renseignement est une chasse jalousement gardée des Etats, la qualité des informations collectées permettant l'anticipation dans la réflexion et la planification, indispensables au succès de la manœuvre future.
Discipline donc majeure, il doit faire l'objet des efforts requis, que ce soit en matière de Recherche et Développement (R&D), de Recherche et Technologie (R&T), de production industrielle et de formation du potentiel humain. Trois volets selon nous devraient recevoir un traitement prioritaire en raison de leur caractère critique :

- les enseignements récents, dans les Balkans, en Afghanistan et en Afrique, sur terre, dans les airs et sur mer, confirment à nouveau l'impérieuse nécessité de disposer d'un renseignement fiable en temps réel pour la planification et la conduite des missions, livrable par **drones.** Cette carence capacitaire contraint actuellement certains Etats membres engagés sur les théâtres du moment à des acquisitions *« sur étagère »* pour faire face à l'urgence, accroissant *de facto* la dépendance de l'Union vis-à-vis des quelques Etats tiers, aujourd'hui seuls pourvoyeurs de ce type d'équipements. Il est difficile de comprendre la paralysie européenne dans ce domaine, alors que les compétences et capacités technologiques existent au sein des entreprises concernées ; par ailleurs, dans un contexte où sécurité extérieure et intérieure se recouvrent, la capacité « drone » répond à un besoin dual, également dirigé contre une grande criminalité alimentant souvent des mouvements armés auxquels les forces militaires sont confrontés sur les théâtres d'opérations.
  Le niveau politique en décembre peut donc donner immédiatement une vigoureuse impulsion à un **programme européen de drones,** capables d'opérer à moyenne altitude et de longue Endurance **(MALE),** utilisables en mode dual**,** avec à terme, la perspective de mise en œuvre d'**une flotte européenne**.

- L'efficacité de l'INTCEN (centre de renseignement), successeur du SITCEN (centre de Situation)

repose sur le flux d'informations que les Etats-membres acceptent de partager. Un **coordonnateur européen du renseignement**, à l'image de celui placé auprès du Conseil pour la lutte contre le terrorisme, pourrait être institué ainsi avec profit. Une phase ultérieure consisterait à bâtir un **service du renseignement européen**, doté de capacités de traitement coordonnées dans les domaines intéressant la sécurité intérieure et extérieure de l'Union.

- En matière de formation, **un programme européen de perfectionnement** en matière de renseignement au profit des experts du domaine pourrait être établi, par exemple dans la cadre du Collège européen de sécurité et de défense (CESD), en complément des formations nationales bien entendu. A cet égard, il ne faut pas négliger les effets d'une **coopération avec l'OTAN**, à condition que les difficultés d'ordre politique affectant les relations entre certains membres des deux organisations puissent naturellement être aplanies.

Le deuxième volet que nous voudrions traiter est celui de la cybersécurité et de la défense.

Les dossiers sensibles que sont cyber sécurité/cyber défense et auxquels cette assemblée s'est déjà intéressée en novembre 2012 ont notablement évolué depuis la parution du document sur la stratégie de l'Union. Porteur de progrès, le cyberespace a parallèlement généré de nouveaux risques, notamment pour les infrastructures critiques nationales et communautaires. Très lié à la problématique du renseignement précédemment évoquée, le cyberespace est un théâtre d'opérations virtuel où l'adversaire, sans visage, est capable d'intrusions de plus en plus sophistiquées, dans un contexte juridique où le phasage paix-crise-guerre se révèle désormais très délicat à définir.

L'Union ne semble ainsi pas avoir d'autre alternative que d'insister sur **une cyber-stratégie européenne** où cyber-défense et lutte contre la cybercriminalité sont étroitement imbriquées. Il s'agit notamment d'inciter les acteurs publics et privés à se protéger par une meilleure information sur les risques encourus et d'instituer là encore un **coordonnateur à la cyber-sécurité** qui s'attacherait à la rationalisation des actions en matière de recherche, de politique industrielle et de sécurité des systèmes d'information, encore trop souvent conduites en ordre dispersé par les Etats-membres et les institutions. Son programme reposerait sur quatre piliers :

- **La cohérence**, qui concilie les notions de liberté et de sécurité, et permet d'harmoniser les politiques, appuyées sur les outils juridiques existants et à venir *[Convention de Budapest sur la cybercriminalité (2001), instrument international contraignant, la directive sur la cybercriminalité (2012)]*.

- **La coordination,** qui est une condition essentielle de succès, qu'elle s'applique à l'intergouvernemental, à l'institutionnel *[Commission, groupe interservices du SEAE, Conseil, agences ou structures spécifiques telles que l'ENISA ou EUROPOL*], entre les Etats et l'Union, entre secteurs public et privé, afin d'éviter les brèches du dispositif et les duplications coûteuses. Le coordonnateur à la cyber-sécurité trouverait ici sa pleine justification. Le Comité politique et de sécurité (COPS) pourrait pour sa part désigner des points de contact chargés du suivi de la cyber-sécurité/cyber-défense.

- **La coopération,** corollaire de la coordination et de la cohérence, implique une politique volontariste d'échange de renseignements entre Etats et en liaison avec d'autres structures pertinentes telles que le centre d'excellence (COE) de l'OTAN en matière de cyber-défense, EUROPOL ou l'ENISA.

- **S'agissant des capacités**, il convient de soutenir au-delà des mots, les programmes existants

ou en voie d'élaboration, en leur donnant réellement les moyens financiers et humains d'aboutir :

- au plan conceptuel, notamment s'agissant des études menées à l'Etat-major de l'Union européenne (EMUE) ;
- en matière de formation aux technologies de l'information et de la communication (TIC) mais aussi des systèmes de sécurité d'information (SSI) ;
- au plan opérationnel**,** par la systématisation des CERT (Computer Emergency Response Team/Equipe d'intervention informatique d'urgence) et par la mise en place d'un volet Défense au Centre européen de lutte contre la cybercriminalité (EC3) récemment créé ;
- en matière de recherche et développement (R&D), par un soutien plus concret à l'Agence Européenne de Défense (AED) dans la conduite de ses missions ;
- au plan industriel, par une promotion active, voire proactive des secteurs de la cyber-sécurité et des CIS, s'appuyant sur l'activité de la Commission dans le cadre de la *« Task Force Défense ».*

Pour conclure, nous proposons quelques suggestions complémentaires qui nous paraîtraient perceptibles par le citoyen et qui témoigneraient d'une volonté de l'Union en matière de défense et de sécurité.

1. Sur les exemples de Weimar ou Weimar Plus, mais aussi des coopérations nordiques ou baltiques, **recherche systématique de nouvelles coopérations structurées permanentes,** dépassant la facilité consistant à qualifier d'européennes les coopérations bilatérales, qui n'en restent pourtant pas moins très utiles.

2. Dotation de la PSDC d'un budget à la hauteur de ses ambitions en orientant les efforts, à commencer par une meilleure répartition des lignes budgétaires dont 20% pour mémoire portent actuellement sur les équipements - 20 % seulement.

3. Préservation et développement d'une industrie de défense européenne performante, s'appuyant pleinement sur les outils existants :

- **.** en dotant l'AED d'un budget qui lui permette vraiment de remplir sa mission au travers de ses 4 fonctions *[développement des capacités de défense, promotion de la R&T en matière de défense, promotion de la coopération en matière d'équipements, création d'un marché européen d'équipements de défense et renforcement de la Base industrielle et technologique de défense européenne (BITDE)] ;*

. en dialogue avec les initiatives développées dans le cadre de l'OCCAR (*Organisation Conjointe de Coopération en matière d'Armement*) et de la LoI (*Letter of Intent*) ;

. en pressant le processus de mutualisation induit par l'initiative *Pooling & Sharing*, conjugué à une coopération équilibrée avec l'OTAN, spécialement pour les capacités manquantes révélées lors des opérations les plus récentes *[le ravitaillement en vol, le renseignement, la cyber-sécurité/défense et le transport stratégique];*

. en s'attachant le plus possible à la dualité de programmes susceptibles d'un emploi civil/militaire, donc tournés vers la sécurité intérieure/extérieure .

4. Identification systématique de **programmes d'actions communs,** lorsque l'initiative individuelle ne s'avère plus possible au regard des enjeux et des moyens requis et disponibles *[notamment cybercriminalité, terrorisme, gestion de conflits lointains et majeurs].*

5. La création d'un centre de planification et de conduite permanent des opérations de l'UE ayant été source de difficultés par le passé, la situation internationale ne nous en presse pas moins d'**identifier des solutions plus permanentes** que celles mises en place de manière empirique sous l'effet de l'urgence, particulièrement lorsque l'OTAN ne peut ni ne veut s'engager.

6. Inscription formelle de l'état-major du Corps européen au titre des instruments de la PSDC ; associant cinq Etats-membres de l'Union, il est l'exemple même de coopération structurée permanente.

7. Recours opérationnel prioritaire futur aux **groupements tactiques** existants ainsi qu'à la **Brigade franco-allemande** (BFA-D/F Brigade), qui, pour mémoire, n'a jamais pu être engagée encore en opération tous moyens réunis depuis sa création en 1989.

8. Association systématique du Parlement européen, pour amener le débat sur les questions de défense et de sécurité à la portée des citoyens par une communication compréhensible de tous, lui conférant de ce fait une légitimité effective accrue dans ce domaine.

Ces suggestions, dont la majeure partie ont un caractère opérationnel n'en n'ont pas moins une portée politique, ce qui nous renvoie maintenant plus particulièrement à ce volet avec l'intervention de l'Ambassadeur Morel. »