CEIS

Le Système d'Information des Armées (SIA)

Le programme SIA : changement de paradigme pour l'armée du futur

Olivia Cahuzac

Pierre Goetz

Sous la direction du G^{al} (2S) Christian Cosquer

Décembre 2013

Les notes stratégiques

LES NOTES STRATÉGIQUES

CEIS est une société de conseil en stratégie et en management des risques. Notre vocation est d'assister nos clients dans leur développement en France et à l'international et de contribuer à la protection de leurs intérêts. Pour cela, nous associons systématiquement vision prospective et approche opérationnelle, maîtrise des informations utiles à la décision et accompagnement dans l'action.

Le Bureau Européen de CEIS conseille et assiste les acteurs publics, européens ou nationaux, ainsi que les acteurs privés dans l'élaboration de leur stratégie européenne, notamment sur les problématiques de défense, sécurité, transport, énergie et affaires maritimes.

Implanté à Bruxelles, le Bureau Européen participe également à des projets européens dans ces domaines.

Les missions du Bureau Européen de CEIS sont les suivantes :

- **Etudes et Analyses :** Etudes de faisabilité, études sur les enjeux et perspectives, cartographie des acteurs, conseil et accompagnement au niveau européen,
- **Ingénierie et management de projets :** Bureau Européen de CEIS conduit et participe également à des projets européens dans ses domaines de compétence,
- **Organisation de groupes de réflexions et d'une conférence annuelle sur la sécurité et la défense :** Conception, organisation et animation d'événements ponctuels ou de réseaux de coopération et d'échanges mixant institutions et entreprises.

Pour mener à bien l'ensemble de ces missions, l'équipe s'appuie sur un réseau européen de contacts, d'experts et de partenaires.

Contact : CEIS Bureau Européen
Axel Dyèvre – Directeur
Boulevard Charlemagne, 42
1000 Bruxelles – Belgique
Tél. : +32 2 646 70 43
adyevre@ceis.eu
http://www.ceis.eu/fr/bureau-europeen

Les idées et opinions exprimées dans ce document n'engagent que les auteurs et ne reflètent pas nécessairement la position de la Société CEIS.

Sommaire

Introduction

Le Système d'Information des Armées ou SIA est un programme de transformation d'une grande partie des systèmes d'information du ministère de la Défense.

Sa mise en place va permettre de mettre à disposition des forces un ensemble cohérent de moyens de gestion de l'information permettant d'assurer la fonction de commandement - remontée des informations et envoi des ordres -, de gérer et d'exploiter les renseignements recueillis, et de suivre l'acheminement des ressources.

A terme, la Défense disposera d'un système unique de commandement et de conduite des opérations ce qui facilitera les échanges d'informations à tous les niveaux.

Les avantages d'un tel dispositif sont nombreux. Tout d'abord, et par définition, il améliorera l'interopérabilité des différents systèmes utilisés par les Armées. Il devrait par ailleurs permettre de réaliser des économies d'échelle en agrégeant les besoins par grandes fonctions opérationnelles et non plus par métier. Il facilitera enfin l'adoption de technologies pertinentes issues du civil, à la pointe de l'innovation.

Ces gains seront rendus possibles grâce à un véritable changement de paradigme. En effet, le SIA est moins un nouveau système qu'une nouvelle façon de penser, de comprendre, de gérer et de construire les systèmes d'information du futur.

Son adoption a nécessité trois bouleversements majeurs:

- le renversement de la logique d'acquisition,
- le passage d'une approche métier à une approche fonction,
- le passage d'une gestion éclatée à une gestion centralisée.

Ces trois bouleversements, qui caractérisent ce que l'on pourrait appeler la logique SIA, vont bien au delà de la mise en place d'un nouveau système d'information. La pérennité de cette logique nécessitait de rapprocher utilisateurs et concepteurs du SIA des potentiels fournisseurs de solutions à intégrer au système en gestation. Conscient de cette nécessité, le ministère de la Défense a créé un concept innovant pour y répondre: le SIA Lab.

Le Système d'Information des Armées : la nécessaire adaptation aux défis du XXIème siècle

A. L'identification de nouveaux besoins : rationalisation, interopérabilité et maîtrise de l'information

La mise en place d'un nouveau Système d'Information des Armées (SIA), harmonisé et interarmées, est le fruit de plusieurs constats sur l'évolution du contexte dans lequel se placent nos Armées, ainsi que de l'identification de besoins nouveaux.

1. L'exigence de systèmes interopérables

L'interopérabilité technique des systèmes d'information est primordiale pour permettre, à un nombre toujours plus grand d'acteurs, le partage des connaissances nécessaires au cycle décisionnel : connaissance de la situation, conception, décision, planification, élaboration et exploitation des ordres. Ces éléments permettent de définir la meilleure stratégie opérationnelle en direct et malgré la pression du temps. Les systèmes d'information et de communication doivent également permettre d'interconnecter les fonctions opérationnelles pour ce qui concerne leurs capacités d'obtention, de traitement et d'échange des informations sur les adversaires, les menaces et l'environnement.

Le concept d'interopérabilité, qu'il est de plus en plus souvent nécessaire d'étendre au-delà de la sphère militaire afin de prendre en compte des organisations civiles, gouvernementales ou non, se décline à plusieurs niveaux :

- doctrinal (harmonisation des concepts d'emploi) ;
- procédural (procédures communes) ;
- organisationnel (structures de commandement) ;
- technique (standardisation des équipements, normes, formats).

2. Une rationalisation nécessaire

Le contexte financier restreint est une des raisons majeures à la promotion d'un système d'information unique au sein du ministère de la Défense. L'objectif recherché est notamment de faire des économies d'échelle en changeant la manière dont le ministère acquiert ses systèmes d'information, en rationalisant

les besoins et, in fine, de réduire les coûts de maintien en condition opérationnelle. « *Dans un contexte de réduction des effectifs, le ministère n'a plus les moyens d'entretenir [une architecture] d'une telle complexité* »[1]. Il convenait donc de rationaliser des systèmes qui s'étaient multipliés au cours des dernières décennies, répondant à des besoins ponctuels et très spécialisés, créant un ensemble complexe de systèmes souvent peu interopérables.

3. Poursuite de la numérisation de l'espace opérationnel et de la maîtrise de l'information

La maîtrise de l'information est devenue centrale dans les opérations militaires, comme le rappelait le Livre Blanc de 2008: « *La maîtrise de l'information repose sur quatre piliers : la transmission de l'information en temps utile, permettant de relier les centres de décision et d'exécution grâce à des débits suffisants ; l'interopérabilité des réseaux d'information, qui optimise la circulation de l'information ; la protection de l'information, ou sécurité des systèmes d'information, qui permet d'assurer la confidentialité, la disponibilité et l'intégrité du système et de l'information traitée ; la vérification de l'information, de sa fiabilité et de sa bonne circulation, ainsi que sa valorisation*[2] ».

En effet, les opérations en réseau ou en coalition demandent de pouvoir partager l'information mais aussi de la protéger car « *le besoin de mettre en commun s'oppose au besoin d'en connaître*.» [3]

Dans cette optique, le projet de numérisation de l'espace de bataille (NEB) au profit de l'armée de Terre a été lancé par le ministère de la Défense en 1999, et est devenu « *un outil indispensable au commandement pour la conduite des opérations*[4] ». Le programme SIA pour les Armées, puis le programme SCORPION[5] pour l'armée de Terre ont été lancés par la suite pour compléter la numérisation et la modernisation des Armées. Dans le même temps, la doctrine a également pris en compte la numérisation progressive des opérations[6].

---

[1] Le Système d'Information des Armées, une nouvelle approche pour des grands systèmes, C. Salomon, CAIA, le magazine des Ingénieurs de l'Armement, N°10D, février 2013
[2] Livre Blanc sur la défense et la sécurité nationale, 2008
[3] Centre de doctrine d'emploi des forces, Principes d'emploi de la FOT numérisée de niveau 3, n°000785/DEF/CDEF/DEO, 8 juillet 2004, p.9
[4] http://www.gouvernement.fr/gouvernement/la-numerisation-de-l-espace-de-bataille-novembre-2012
[5] Programme Scorpion, Ministère de la Défense
[6] Centre de doctrine d'emploi des forces, Principes d'emploi de la FOT numérisée de niveau 3, n°000785/DEF/CDEF/DEO, 8 juillet 2004, p.9

4. Assurer la rupture stratégique

Les systèmes d'information opérationnels et de communication (SIOC) doivent également garantir la disponibilité, la continuité, la pertinence et la protection de l'information nécessaire à l'exercice des cinq fonctions stratégiques (connaissance et anticipation, dissuasion, protection, prévention, intervention). Par exemple, en ce qui concerne la fonction stratégique « connaissance et anticipation », les systèmes d'information doivent permettre de soutenir la chaine de commandement dans l'aide à la décision, de maîtriser l'information ou encore de contrôler l'action. Le Livre Blanc sur la défense et la sécurité nationale de 2008 rappelait ainsi « *qu'au niveau stratégique, l'objectif [des systèmes d'information] est de mettre en réseau tous les responsables intéressés, afin d'éclairer la prise de décision*[7] ».

Enfin, la capacité d'entrée en premier constitue l'un des facteurs de puissance essentiels pour maintenir une place comme acteur militaire de premier plan. Les capacités C4ISR[8] au niveau stratégique, opératif et tactique permettent à la nation-cadre d'assurer la direction de la consultation politico-militaire, de la planification et de la conduite des opérations. En effet, « *pour pouvoir prétendre vouloir jouer les premiers rôles au sein d'une coalition multinationale [un pays] doit posséder une gamme complète de SIC performants, sécurisés et interopérables (…). La maîtrise des SIC est un facteur de puissance militaire et de crédibilité sur la scène internationale*[9] ».

Lancé en 2010 et prévu pour une mise en service opérationnel à partir de 2016, le SIA contribuera à rendre ces différentes briques de systèmes d'information interopérables et harmonisées, afin d'assurer une complète maîtrise de l'information par les Armées. En ce sens, ce programme contribuera à garantir l'exercice des cinq fonctions stratégiques.

---

[7] Livre Blanc sur la défense et la sécurité nationale, 2008
[8] Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
[9] Les systèmes d'information et de communication, un domaine sous-estimé au Coeur des operations militaires modernes, LCL Stéphane Bannier, Revue de la Défense national N°750-ai 2012

B. La nécessaire adaptation de la sphère militaire aux derniers développements des TIC

1. Vers une nouvelle démarche capacitaire

Jusqu'à présent, l'acquisition et le développement de nouvelles technologies ou de grands programmes d'armement se sont fait sur des cycles souvent longs. Les décennies précédentes ont montré que l'Etat a souvent privilégié une relation en bilatéral avec un ou deux maîtres d'œuvre. Ceci a entrainé « *un effet d'éviction pour d'éventuels nouveaux entrants, le ticket d'entrée étant trop élevé, (…) ainsi qu'une explosion des coûts*[10] ».

D'autre part, les innovations dans le domaine des systèmes d'information et des nouvelles technologies ne peuvent plus se permettre d'effet tunnel. Pour garder une avance sur le plan technologique, le ministère de la Défense a donc adapté sa stratégie d'acquisition et favorisé une approche flexible, via l'acquisition de technologies et d'applications dans des cycles courts, sur le modèle des technologies civiles. Dans le domaine des systèmes d'information, l'adaptation incrémentale des systèmes semble être l'approche la plus adaptée.

2. Répondre aux décrochages des technologies militaires par rapport aux technologies civiles

La logique du SIA vise également à prendre en compte un nouveau développement : si jusqu'à présent les technologies militaires faisaient figure de référence avant d'être ensuite adoptées et adaptées par le monde civil, la tendance s'est inversée depuis quelques années.

C'est particulièrement vrai en ce qui concerne les nouvelles technologies de l'information et des communications, tirées par le marché. Dans ce secteur, les cycles de développement des produits civils sont souvent très courts. Le secteur militaire, soumis à d'autres contraintes capacitaires – sécurité des systèmes, approvisionnement et maintien en condition opérationnelle notamment – ne peut suivre un tel rythme. Dans ce contexte, il y a donc un réel risque de décrochage voire de perte de pertinence par l'adoption de technologies devenues

[10] CAIA, février 2013, ibid.

obsolètes une fois leur mise en œuvre effective.[11]

Cela serait d'autant plus regrettable que bon nombre de technologies dites civiles pourraient être en mesure d'apporter une réponse immédiate et satisfaisante à un grand nombre de besoins militaires. Le ministère de la Défense souhaitait donc être en mesure, le cas échéant, d'adapter et d'adopter des produits civils ayant des fonctionnalités et des spécifications utiles au secteur militaire. C'est justement l'un des objectifs affichés des concepteurs du SIA. Cette approche est d'autant plus pertinente que l'adoption de ces technologies civiles ne nécessite pas un effort important si ce n'est une veille efficace et réactive sur leurs émergences et sur leurs utilisations potentielles dans le cadre de systèmes de défense.

3. Répondre aux attentes et aux besoins des utilisateurs

Les développements observés dans le monde civil ne sont pas anodins. Ils ont un impact sur les attentes et les habitudes prises par les utilisateurs, et en particulier ceux de la nouvelle génération parmi lesquels se retrouvent également les futurs utilisateurs des systèmes d'information de la Défense.

Très tôt dotés de terminaux mobiles, ces utilisateurs sont très exigeants et pratiques. Ils cherchent une application qui remplit une fonctionnalité bien précise et n'hésitent pas à l'abandonner après quelques essais pour une autre jugée plus performante. Ce comportement est facilité par la disponibilité sur le marché de toute une palette d'applications compétitives et l'accès aisé aux analyses comparatives.

Par ailleurs, en matière de nouvelles technologies, la complexité n'est plus forcément perçue comme un gage de sérieux ou de fiabilité. Bien au contraire, les utilisateurs privilégient les solutions fonctionnant intuitivement et qui font disparaître les aspects techniques complexes de l'application sous une interface épurée. L'ergonomie et l'esthétique sont devenus les maîtres mots, comme en témoigne par exemple le succès de l'iPhone.

Ainsi, face à de futurs utilisateurs exigeants et ayant déjà accès à des systèmes de communication à la fois simples d'utilisation et performants, le ministère de la Défense a souhaité repenser son approche. La logique du SIA, qui vise à l'intégration d'applications tierces, le cas échéant issues du monde civil, constitue une réponse à ces attentes.

Cette logique est d'autant plus pertinente que les risques en termes de sécurité

[11] Technologies duales et défense, entre politique et management, Jean-François Daguzan, Fondation pour la Recherche Stratégique

ne sont pas nuls. En effet, bon nombre d'utilisateurs pourraient être tentés de contourner les systèmes de communication professionnels, ultra-sécurisés mais peu pratiques, au moyen de technologies grand public aux fonctions équivalentes et faciles d'utilisation, mais beaucoup plus vulnérables en termes de sécurité. Il est donc essentiel pour tous les secteurs d'activités sensibles, et en particulier pour la Défense, de mettre à disposition de son personnel des outils de communication fiables et au fonctionnement intuitif. Cela permettra de limiter les tentations de recours en parallèle à des technologies grand public moins sécurisées, mais plus faciles à utiliser et remplissant les mêmes fonctions.

C. Cadre et objectifs du SIA

« *Le principal intérêt du SIA, c'est surtout la démarche, qui a fait exploser les canons habituels de la conduite des programmes d'armement, que ce soit en termes d'expression du besoin, de stratégie d'acquisition ou de politique industrielle*[12] ».

1. La valorisation du rôle central des systèmes d'information

La Loi de Programmation Militaire 2014-2019 rappelle la place centrale que tiendra à terme le Système d'information des armées (SIA). « *Le SIA s'inscrit dans l'environnement des systèmes d'information du ministère de la Défense. Il constitue l'outil de commandement des armées et doit permettre aux forces françaises de planifier, préparer et conduire les opérations grâce à une gestion de l'information optimisée, favorisant la coopération interarmées et interalliée*[13] ».

Afin de valoriser la place centrale des systèmes d'information, une démarche de restructuration, de convergence et d'optimisation des systèmes existants a été entamée par le ministère de la Défense.

Le SIA, piloté par la Direction Générale de l'Armement (DGA) est ainsi entré en phase de conception début 2010. Un premier niveau de capacité opérationnelle sera mis en service en 2016, et l'ensemble des composants constituant la première version du SIA seront livrés en 2017, pour évoluer jusqu'en 2030. Le

[12] CAIA, février 2013, ibid.
[13] Loi de Programmation Militaire 2014-2020

ministère de la Défense vise 30 000 utilisateurs directs du SIA[14]. Le programme a été financé à hauteur de 46,6 millions d'euros en 2013[15].

2. D'une logique « métier » à une logique « fonction » : la mise en place d'un socle technique interarmées (STC-IA)

La démarche suivie pour le SIA repose sur la définition de trois éléments: une architecture cible, un socle technique et des services communs appelés à terme à devenir le cadre unique d'environnement des systèmes d'information opérationnels (STC-IA).

En effet, les systèmes d'information opérationnels utilisent, lorsque c'est possible, des composants similaires aux systèmes d'information d'usage général. Ceux-ci seront le cas échéant adaptés pour satisfaire aux contraintes des opérations militaires (qualité, sécurité). Dès lors que ces composants logiciels et/ou techniques seront communs et qu'ils présenteront une vocation générale, ils entreront formellement dans une architecture globale appelée « socle ».

Les socles techniques existants doivent converger vers ce cadre unique, permettant ainsi à la Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information (DIRISI), sur le territoire national et sur l'ensemble des théâtres opérationnels, de rationaliser ses moyens et ses ressources d'administration. *« Idéalement, à une fonction donnée devrait correspondre une application informatique unique[16] ».*

[14] CAIA, février 2013, ibid.
[15] Avis n°150 du Sénat, présenté au nom de la commission des affaires étrangères, de la défense et des forces armées sur le projet de loi de finances pour 2013 – Tome VIII Défense : Equipement des forces, par MM. Daniel Reiner, Xavier Pintat et Jacques Gautier.
[16] Acteurs publics – Version de travail, projet de rapport d'information du Sénat, Septembre 2013

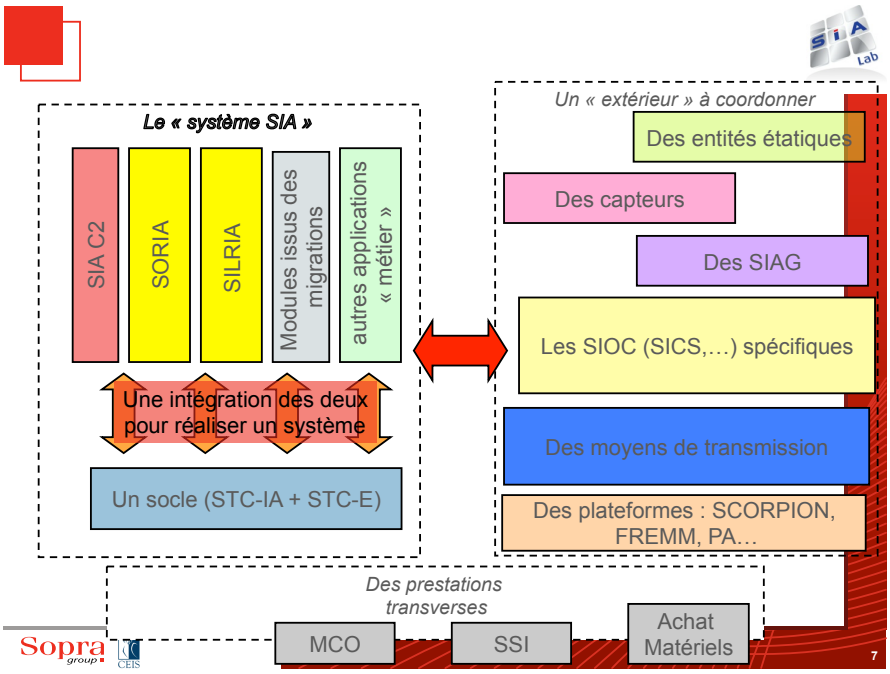

Figure 1 - La logique SIA (Source : SIA Lab)

Ce « socle », qui a vocation à être déployé sur les intranets métropolitains, de théâtre et sur les plateformes navales, doit être capable d'intégrer des solutions techniques tierces (ministérielle, OTAN, UE) pour répondre aux besoins des Armées.

Sur le plan industriel, le ministère de la Défense a modifié son approche en ouvrant la définition du SIA à un large panel d'industriels. Cette démarche contribuera notamment à la flexibilité du réseau qui se construira par petits pas, ainsi qu'à l'ouverture de l'accès aux marchés de la défense à différents types d'acteurs, notamment aux grands maîtres d'œuvre, aux Entreprises de Services Numériques (ESN) et aux Petites et Moyennes Entreprises (PME)[17].

[17] CAIA, février 2013, ibid.

Le SIA : bénéfices escomptés et défis de mise en œuvre

A. La plus-value du SIA dans la gestion et la prise de décision

La mise en œuvre de la logique SIA, aura des conséquences à tous les niveaux de décision et de mise en œuvre.

1. Au niveau politique : un meilleur contrôle des dépenses et une marge de manœuvre renforcée dans un cadre d'opération multinational

Au niveau politique, l'adoption d'une plateforme unique sur laquelle viendront se greffer des applications compatibles entre elles permettra d'avoir une meilleure visibilité sur les coûts engendrés par le système. En effet, la mise en œuvre du SIA ne nécessitera pas la prise en charge d'un large pan du système par un grand maître d'œuvre industriel unique, avec les risques en termes de dépassement de coûts et de calendrier que cela peut occasionner. Au contraire, la stratégie d'acquisition morcelée de modules à intégrer sur une plateforme commune permettra de mieux mesurer les dépenses consenties au coup par coup[18]. Au final, le coût global de la fonction SIC au sein du ministère de la Défense devrait considérablement diminuer.

Par ailleurs, les conséquences de la remise en cause d'un choix fait à un moment donné seront limitées : il ne sera plus nécessaire de prendre la lourde responsabilité d'abandonner un système entier mais simplement d'adapter ou de remplacer les briques – moins onéreuses - du système SIA ne donnant pas entière satisfaction.

Les décideurs politiques bénéficieront également des améliorations apportées par l'interopérabilité du système.

Le système SIA est, de plus, construit autour de solutions compatibles avec celles mises en œuvre au sein de l'Alliance, en tirant partie, avec pertinence, des solutions développées par l'OTAN. Cela devrait grandement faciliter la coopération avec les Alliés dans les cadres multinationaux (UE, Otan) qui sont

[18] CAIA, février 2013, ibid.

devenus la règle plutôt que l'exception. De même, le système SIA pourra devenir le cadre de promotion de solutions nationales auprès de l'Alliance.

2. Une gestion centralisée

La maîtrise de l'information est une des conditions du succès des opérations. Notamment, la maîtrise du processus décisionnel permet d'élaborer, de conduire ou de faire évoluer les actions validées. Cette maîtrise de l'information est également caractérisée par la qualité, le partage, la valorisation de l'information et la qualité de service des réseaux.

L'amélioration de ces facteurs dépend, pour une grande part, de la performance atteinte dans la gestion de l'information. Celle-ci exige notamment :

- une capacité à organiser et formaliser la connaissance,
- une capacité à gérer les accès,
- une capacité à assurer l'intégrité, la confidentialité et la disponibilité des données et des processus du système (sécurité),
- une capacité à gérer dynamiquement la diffusion des flux de données.

La DIRISI, opérateur ministériel des SIC, aura un rôle central dans la supervision de ces capacités, ceci en parallèle des théâtres d'opérations avec le niveau de subsidiarité adéquat.

B. La plus-value du SIA aux niveaux technique et opérationnel

1. Au niveau technique : combler le retard avec les technologies civiles

Sur le plan technique, l'adoption de l'approche SIA devrait permettre une réduction drastique des cycles de développement. En matière de systèmes d'information, et au vu de ses spécificités, le secteur militaire accuse parfois un retard par rapport au monde civil. Parmi les raisons invoquées figurent « *la logique programmatique, la difficulté de préciser le besoin opérationnel, la volonté industrielle de pérenniser certains grands programmes, une communication parfois peu claire sur les objectifs à atteindre et une utilisation réduite des organismes de pilotage*[19] ».

[19] Centre de doctrine d'emploi des forces, Principes d'emploi de la FOT numérisée de niveau 3, n°000785/DEF/CDEF/DEO, 8 juillet 2004, p.9

Les problématiques SIC ont également été souvent considérées en marge du processus de planification du Ministère de la défense. En effet, « *dans la mesure où la maîtrise du temps est un facteur déterminant, des adaptations lourdes du dispositif SIC peuvent entrainer des retards inacceptables dans le tempo des opérations*[20] ».

La logique SIA vise donc à combler ces lacunes en proposant une plateforme unique capable d'intégrer très rapidement les nouvelles technologies, en particulier celles qui sont issues du domaine civil. Plus encore, le SIA permettra de rendre interopérables les différentes applications choisies. Jusqu'à présent, si les systèmes retenus ont globalement donné satisfaction dans tel ou tel contexte, le manque d'interopérabilité a souvent été pointé du doigt. La logique SIA permettra de progresser également dans ce domaine.

2. Au niveau opérationnel : un système cohérent, facilitant l'interopérabilité et devant répondre à des besoins capacitaires

C'est sans doute sur le plan opérationnel que les changements induits par le SIA seront les plus sensibles. Le SIA doit permettre de décloisonner les échanges entre les opérationnels et de passer d'une logique de milieu (systèmes différents et cloisonnés par armées) à une logique de fonction.

En d'autres termes, il s'agira de mettre fin au mode de fonctionnement en silos, chaque armée possédant son ou ses systèmes propres, développés sans réel souci d'interopérabilité et fonctionnant de manière indépendante. Grâce au SIA cet agrégat sera remplacé par un système cohérent, articulé autour de fonctions métiers communes à savoir : le Renseignement, le Commandement des opérations, l'Entraînement des forces, l'Etude du milieu et la Logistique.

Le système permettra concrètement:

- de remonter très rapidement des informations en provenance des théâtres d'opération et à destination des niveaux décisionnels,
- de faciliter la synthèse des informations sur une situation donnée,
- d'exploiter au mieux les renseignements recueillis,
- le cas échéant, de faciliter le travail collaboratif en permettant les échanges entre systèmes.

En somme, la Défense disposera d'un unique système de commandement et de contrôle des opérations, facilitant les échanges à tous les niveaux. Cela devrait se traduire par une amélioration notable des performances grâce à la réduction

[20] Les systèmes d'information et de communication, un domaine sous-estimé au Coeur des operations militaires modernes, LCL Stéphane Bannier, Revue de la Défense national N°750-ai 2012

du nombre de systèmes et à l'utilisation transversale de la plupart d'entre eux.

In fine, le SIA facilitera également le travail en coalition et permettra de combler les lacunes existantes dans ce domaine. L'un des exemples récents souvent cités est l'opération en Libye, qui a mis en lumière la difficulté de faire fonctionner les systèmes d'information français existants avec ceux des Alliés[21].

3. Au niveau opérationnel : la possibilité de mettre en place un système plus ergonomique

L'enjeu du SIA est également de conserver une capacité militaire à maîtriser les SIOC indispensables à la conduite des opérations. Cette capacité étant fragile, notamment aux niveaux tactiques, le système SIA doit apporter une grande facilité pour l'opérateur tant dans son déploiement que dans son administration.

Au-delà des seuls militaires français amenés à utiliser les SIOC dans le cadre de leurs responsabilités, des membres d'autres pays - au premier rang desquels les pays membres de l'OTAN - sont à mêmes de pouvoir utiliser les SIOC nationaux. L'enjeu est que ces personnels puissent s'approprier très rapidement les fonctions principales des SIOC et les utiliser, y compris sous fortes contraintes de stress, sans devoir recourir à de longues périodes de familiarisation. Les solutions mises en œuvre dans le SIA doivent donc être proches de celles employées couramment dans le monde civil et de celles mises en œuvre dans les systèmes de l'OTAN. Le SIA est construit autour de standards afin de valoriser la familiarisation du personnel à l'emploi des outils informatiques du marché.

[21] La maîtrise des SIC au sein du ministère de la Défense, Cyber-défense, 30 août 2012

C. Les défis

La bonne mise en œuvre de la logique SIA nécessitera de prendre en compte et de surmonter un certain nombre de défis de natures très différentes. En effet, le Système d'Information des Armées correspondant moins à un nouvel outil qu'à un changement de logique, il doit également prendre en compte des aspects humains au delà des simples défis techniques.

1. Les défis techniques

Une fois mis en place, le SIA permettra de limiter les risques et les coûts en morcelant la demande. Cela étant dit, la création du socle commun sur lequel doivent converger les systèmes existants, est en soi un programme de grande envergure. Cette phase de transition comporte de fait des risques en termes de dépassement de coûts et de non respect des calendriers prévus. Ces risques sont toutefois largement limités par l'adoption d'une approche incrémentale qui se traduit par une mise en service progressive s'étalant de 2012 à 2017. En pratique, la migration vers le nouveau système s'opérera en deux grandes étapes : la convergence des socles sur lesquels reposent les systèmes (SIA V0) puis l'optimisation des socles et la réorganisation des applications au travers d'une démarche d'urbanisation[22]. Par ailleurs, en consultant et en impliquant les principales parties prenantes – notamment par le biais des « fédérations SIA » des trois Armées – les concepteurs du système en facilitent la mise en œuvre et l'appropriation par ses utilisateurs finaux.

Sur le plan technique, le SIA se concentre pour l'instant sur les niveaux stratégique et opératif. Certains observateurs soulignent qu'il reste à démontrer que l'interconnexion pourra se faire de manière satisfaisante avec les systèmes utilisés au niveau tactique[23].

2. Faire face à des cyber menaces de plus en plus présentes

Parmi les besoins que le système SIA doit pouvoir prendre en compte rapidement, figure celui de la sécurité des systèmes d'information. L'enjeu est de pouvoir répondre à un besoin de sécurité dans les conditions réglementaires tout en préservant l'interopérabilité avec les Alliés et les autres acteurs intervenant dans l'action militaire. Cela impose une architecture particulière du système SIA

[22] Objectif directeur des systèmes d'information opérationnels et de communication, Etat Major des Armées, 24 juillet 2007
[23] The transformation of the armed forces : the Forza NEC program, Philippe Gros, IAI Research papers, p.126

et de ses composants permettant d'obtenir une homologation globale dans des délais compatibles avec la réalité des opérations. Notamment, le système SIA doit offrir une structure suffisamment robuste et résistante pour permettre aux SIOC de fonctionner dans des conditions satisfaisantes lors de l'exécution des missions opérationnelles, y compris en cas d'actions nuisibles portées contre lui.

Le niveau de protection obtenu n'est jamais définitif et devra donc être régulièrement réévalué pour faire face à l'évolution constante des cyber menaces. Le système SIA sera conçu pour y répondre.

3. Les défis humains

Il faut également souligner que le changement de logique se décrète moins qu'il ne se met en œuvre après avoir été compris et accepté par les principaux acteurs concernés. En d'autres termes, le changement de paradigme technique devra s'accompagner d'un effort de formation à destination des utilisateurs. En particulier, si le fonctionnement en silos avait de nombreux inconvénients, la rationalisation du système comporte également des risques de sécurité puisque l'information circulera plus facilement. Il conviendra dès lors de sensibiliser les utilisateurs à ces risques, notamment en insistant sur les bonnes pratiques en matière de gestion et de classification de l'information. Les solutions techniques correspondantes devront également être élaborées et adoptées.

Enfin, comme mentionné précédemment, d'autres pays alliés, notamment dans le cadre de l'OTAN, sont à même d'utiliser les SIOC nationaux. L'enjeu est qu'ils puissent s'approprier et utiliser très rapidement les fonctions principales des SIOC. Les solutions mises en œuvre dans le SIA doivent donc être proches de celles employées couramment dans le monde civil et de celles mises en œuvre dans les systèmes de l'OTAN.

4. La pérennisation de l'approche

Pour répondre aux nombreuses attentes qu'elle suscite, la logique SIA suppose de relever un dernier défi qui est celui de l'accès effectif et continu aux technologies de communication civiles, à la fois innovantes et pertinentes pour le secteur de la Défense. En effet, rien ne sert de prévoir un système d'acquisition morcelé et donc non réservé aux grands maîtres d'œuvre industriels, si le lien avec les acteurs de plus petite taille n'est pas réalisé. En d'autres termes, à quoi bon mettre en place un « magasin en ligne, sorte d'« Apple store », si les développeurs n'en connaissent pas l'existence et ne savent pas comment y avoir accès ni comment y présenter leurs produits?

C'est justement à cet aspect crucial pour la mise en œuvre de la logique SIA que

doit s’attacher de répondre le SIA Lab.

Doté d’une infrastructure physique permettant de recevoir des développeurs indépendants et des PME, cet espace de démonstration héberge chaque mois des sessions de présentation de produits et solutions. Ces sessions sont ouvertes aux représentants étatiques concernés. Il s’agit ainsi de détecter et expérimenter des solutions pouvant être déployées facilement sur l'infrastructure déployée du SIA.

Chaque session permet des échanges fructueux et constructifs. Les acteurs étatiques sont en effet mis en contact direct avec les concepteurs des technologies innovantes et peuvent ainsi avoir une vision sans cesse actualisée de l’état de l’art en matière de systèmes d’information. Plus encore, les échanges entre concepteurs des produits et représentants étatiques permettent aux premiers d’être en prise directe avec de potentiels acheteurs et aux seconds de mieux structurer l’offre en faisant directement part de leurs attentes.

CEIS

Déjà parus :

PME et marchés de défense – Le SIA Lab, une initiative au service de l'accès des PME aux marchés de la défense. Octobre 2013

R&D et PME de défense – Le SIA Lab, un outil innovant de mise en valeur de PME. Octobre 2013

De l'Union douanière à l'Union eurasiatique – Etat et perspectives d'intégration dans l'espace post-soviétique. Octobre 2013

Une nouvelle approche du terrorisme – Mieux comprendre le profil des groupes terroristes et de leurs membres. Mai 2013

La coopération technologique et industrielle de défense et de sécurité du Brésil – Un instantané, côté Sud. Mai 2013

Le financement de la R&D de défense par l'Union européenne. Avril 2013

Les drones et la puissance aérienne future. Mars 2013

Nouvelles guerres de l'information : le cas de la Syrie. Novembre 2012

Ariane et l'avenir des lancements spatiaux européens. Août 2012

Le F35/JSF : ambition américaine, mirage européen. Juillet 2012

Compagnie Européenne d'Intelligence
Stratégique (CEIS)
Société Anonyme au capital de 150 510 € - SIRET : 414 881 821
00022 – APE : 741 G

280 boulevard Saint Germain – 75007 Paris
Tél. : 01 45 55 00 20 – Fax : 01 45 55 00 60
Tous droits réservés

LES NOTES STRATÉGIQUES

Les notes σtratégiques