



Berne, le 11 décembre 2020

Armée – Compétences garanties dans les nouvelles technologies

Rapport du Conseil fédéral en exécution du postulat
17.3106 Marcel Dobler du 14 mars 2017

Table des matières

1	Contexte	3
2	Mandat	3
3	Compétences technologiques.....	4
3.1	Administration.....	4
3.2	Base technologique et industrielle importante pour la sécurité.....	5
3.3	Personnel de milice	6
3.4	Personnel professionnel (civil et militaire)	8
4	Collaboration avec les partenaires	9
4.1	Instituts de formation	9
4.2	Économie privée	10
4.3	Coopération internationale	10
5	Conclusion	11

1 Contexte

Jamais dans l'histoire le monde n'a connu d'avancées technologiques aussi rapides qu'aujourd'hui. Aussi, la numérisation – et dès lors la modernisation et la mise en réseau – de tous les systèmes de l'armée a accru l'importance des compétences dans ce domaine. Simultanément, la planification, l'acquisition et l'exploitation de ces moyens deviennent plus exigeantes pour l'armée, notamment parce que les technologies influencent grandement la structure des armées modernes et qu'elles sont indispensables à l'accomplissement de missions bien menées. Le choix des technologies appropriées est essentiel : les systèmes militaires doivent pouvoir être maîtrisés par une armée de milice. Lors de la planification et de l'acquisition de ses moyens d'engagement ainsi que pendant leur exploitation, l'armée est tributaire de compétences techniques et scientifiques pour lui permettre d'évaluer les risques sous l'angle des coûts, de l'utilité et de la vulnérabilité des technologies engagées.

Depuis le dépôt du postulat en 2017, les *Principes du Conseil fédéral en matière de politique d'armement du DDPS* ont été édictés, lesquels se concentrent sur le maintien des compétences technologiques et des capacités industrielles. Pour leur part, le Groupement Défense et l'Office fédéral de l'armement (armasuisse) ont déjà pris diverses mesures visant à atteindre cet objectif, notamment en introduisant le stage de formation cyber, l'*ICT Warrior Academy*, le campus cyberdéfense du DDPS (CYD-Campus) et l'affectation différenciée des conscrits lors du recrutement. Le Groupement Défense et armasuisse analysent et traitent en permanence les aspects de la transformation numérique, les intègrent dans les bases stratégiques et les concrétisent par étape.

2 Mandat

Le 14 mars 2017, le conseiller national Marcel Dobler a déposé le postulat 17.3106 *Armée 2.0. La Suisse doit promouvoir et sauvegarder le savoir-faire technologique*, dont le texte est le suivant :

« Le Conseil fédéral est chargé d'examiner comment l'armée entend satisfaire à long terme ses besoins croissants en termes de compétences dans le domaine des nouvelles technologies. Ce faisant, il tiendra particulièrement compte des objectifs suivants :

1. garantir les effectifs pour satisfaire les besoins en constante augmentation dans le domaine des compétences technologiques et scientifiques ;
2. identifier les besoins en termes de collaborateurs scientifiques et technologiques dans l'armée d'aujourd'hui et dans celle de demain ; les défis toujours plus nombreux dans le cyberspace et l'évolution technologique constituent deux exemples ;
3. collaborer avec les établissements de formation et le monde économique (y compris avec les entreprises de la Confédération, sur le modèle israélien) ;
4. faire évoluer le rôle des militaires : donner la possibilité à des militaires en service long de se consacrer à des activités scientifiques ; allonger la durée des interventions ; comptabiliser comme jours de service les stages scientifiques ou la rédaction de thèses de doctorat ;
5. établir de nouveaux critères pour évaluer l'aptitude au service des détenteurs de connaissances spécifiques (aptitude nuancée) ; instaurer de nouveaux mécanismes d'avancement pour les détenteurs de connaissances qu'il faut maintenir plus longtemps dans le système. »

Le postulat justifie l'accroissement de ces besoins par l'importance croissante des systèmes autonomes, de la défense contre les cyberattaques, de la gestion de l'information et de la garantie de prestations élevées dans le domaine de la communication. L'armée doit se pencher sur cette évolution et sur le transfert du matériel aux logiciels. Il convient en outre de promouvoir la collaboration avec les

instituts de formation et l'économie afin de pouvoir acquérir et conserver longtemps le savoir-faire technologique.

Le Conseil national a adopté le postulat le 16 juin 2017.

3 Compétences technologiques

Les tâches que l'armée doit accomplir (planification des forces et de l'armement, engagement, exploitation et maintenance des systèmes, instruction) exigent chacune un savoir-faire technologique qui leur est spécifique. D'autres domaines ont aussi leur importance. Ils sont présentés ci-après.

3.1 Administration

L'importance des nouvelles technologies et du besoin en savoir-faire qui en résulte n'est pas seulement un défi pour l'armée, mais aussi pour l'administration, d'où l'examen régulier des possibilités de développer ou de mettre à disposition les compétences technologiques et scientifiques nécessaires. Dans sa *Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022* du 18 avril 2018, le Conseil fédéral retient que le développement des compétences et du savoir constitue la base des activités liées aux nouvelles technologies. Celle-ci doit être acquise notamment par la détection précoce des tendances et des technologies, l'élargissement des connaissances ainsi que le développement et la promotion des compétences dans les domaines de la recherche et de la formation. Les *Principes du Conseil fédéral en matière de politique d'armement du DDPS* du 24 octobre 2018 prennent en compte ces aspects et se concentrent sur les besoins en compétences technologiques et en capacités industrielles¹ ainsi que sur les diverses possibilités permettant à la Suisse de couvrir ses besoins.

Dans le domaine de la sécurité, le savoir-faire nécessaire est développé avec des partenaires issus d'organes compétents, qu'ils soient internes ou externes, d'organisations de sécurité nationales ou internationales, du monde des sciences ou de l'industrie. Dans ce contexte, la Confédération (armasuisse, OFPP et DFAE/DP) régit la recherche de l'administration conformément à l'art. 16, al. 1, de la loi fédérale du 14 décembre 2012 sur l'encouragement de la recherche et de l'innovation (LERI)², notamment dans le domaine *Politique de sécurité et de paix*. Dans ce domaine, les recherches menées par armasuisse ont pour but d'assurer l'expertise nécessaire et les compétences scientifiques et technologiques clés dont l'armée et d'autres instruments de la politique de sécurité ont besoin pour disposer durablement des capacités requises³.

Dans le cadre du développement des forces armées et de la planification de l'armement, le Groupement Défense détermine pour chaque domaine des tendances majeures pour lesquelles la technologie est, elle aussi, un des principaux moteurs⁴. Dans ce contexte, armasuisse assure les compétences

¹ Selon les [Principes du Conseil fédéral en matière de politique d'armement du DDPS](#), il faut garantir, à travers la politique d'armement, que l'armée et d'autres institutions chargées de la sécurité de la Confédération reçoivent en temps utile, selon les principes de l'économie et de la transparence, l'équipement, l'armement et les services dont elles ont besoin. Au centre de la politique d'armement, le besoin de connaissances spécialisées critiques, de technologies clés liées à la sécurité, de systèmes complexes, de biens, de constructions et de prestations, de même que la garantie de capacités industrielles clés et de capacités permettant d'assurer la fiabilité du fonctionnement ainsi que l'engagement et la durabilité des systèmes introduits à l'armée.

² RS 420.1

³ Les plans de recherche d'armasuisse, de l'OFPP et du DFAE/DP sont rassemblés dans la [recherche de l'administration dans le domaine de la politique de sécurité et de paix](#) et coordonnés par le Secrétariat d'État à la formation, à la recherche et à l'innovation avec les concepts pluriannuels d'autres domaines politiques.

⁴ Le plan directeur de mise en œuvre de la stratégie informatique de la Confédération 2020-2030 comprend, entre autres, des initiatives stratégiques destinées à soutenir la transformation numérique.

technologiques et scientifiques pour l'armée et le DDPS avec son domaine de compétences Sciences et technologies (S+T) et centre technologique du DDPS. Armasuisse est aussi compétente pour les activités dans le domaine de la recherche appliquée. En se fondant sur une gestion globale des technologies, armasuisse S+T, attribue des mandats de recherche dans le cadre de programmes de recherche⁵ axés sur les besoins de l'armée, et recourt pour ce faire aux réseaux établis avec les universités, les hautes écoles, les instituts ainsi qu'à ceux de l'industrie et de l'administration en Suisse et à l'étranger.

Espaces d'innovation

Actuellement, des espaces d'innovation sont créés au sein du DDPS comme instruments supplémentaires pour mieux aborder les changements permanents qui se produisent dans l'environnement global – en particulier en raison des cycles de production qui ne cessent de se raccourcir. L'espace d'innovation conceptualise un groupe de travail s'occupant d'un thème précis pendant une période donnée et se compose de représentants des utilisateurs, des acquisitions ainsi que d'autres personnes compétentes – le cas échéant externes. Ainsi, des lacunes au niveau des compétences technologiques peuvent par exemple être décelées et le savoir nécessaire développé en conséquence.

Transformation de la Base d'aide au commandement (BAC) en commandement Cyber

Vu les menaces actuelles, le Conseil fédéral entend transformer dès 2024 la BAC en commandement Cyber. La modernisation de tous les systèmes de l'administration militaire et de l'armée implique des exigences élevées pour une architecture informatique uniformisée et impose une standardisation des applications. De plus, avec le développement des réseaux, les défis en matière de cyberprotection augmentent significativement. Afin de mieux répondre à ces exigences, la BAC devra se transformer pour passer d'une organisation de soutien largement diversifiée à un commandement militaire opérationnel. Le commandement Cyber devra fournir les capacités militaires clés dans les domaines de l'image de la situation, de la cyberdéfense, des prestations informatiques, de l'aide au commandement, de la cryptologie et de la guerre électronique.

Concernant le personnel, l'administration militaire est en concurrence avec le marché civil du travail et elle est impactée directement par le manque de spécialistes en informatique. Vu le caractère particulier de leurs activités, les nouveaux collaborateurs de l'administration militaire doivent souvent suivre des cours complets de perfectionnement. Le choix de candidats parmi les formations Cyber de milice ne permet que de réduire partiellement cet effort dans la formation. Le regroupement des capacités et des prestations sous un même commandement présente un avantage sur le plan du recrutement et de la formation d'employés qualifiés.

3.2 Base technologique et industrielle importante pour la sécurité

Le savoir-faire technologique nécessaire à la sécurité de la Suisse ne se développe pas seulement au sein de l'administration et de l'armée. Le renforcement de la base technologique et industrielle importante pour la sécurité (BTIS) est aussi essentiel. Elle doit être en mesure de donner accès à des compétences technologiques et à des capacités industrielles prioritaires avec les moyens nécessaires

⁵ Les programmes de recherche sont : 1) exploration et surveillance, 2) communication, 3) cyberspace et information, 4) effet, protection et sécurité, 5) systèmes mobiles sans pilote, 6) identification précoce des technologies.

basés en Suisse. Pour ce faire, la Confédération dispose, conformément aux *Principes du Conseil fédéral en matière de politique d'armement du DDPS*, de sept instruments de pilotage⁶.

Se référant aux besoins de l'armée, armasuisse S+T a défini les technologies essentielles pour la Suisse. Ces technologies – comme celles de la communication, de l'information et des capteurs – sont obtenues de manière ponctuelle et renforcées en Suisse par un contrôle de la Confédération. Périodiquement, elles sont adaptées en fonction de l'évolution technologique et des besoins de l'armée.

La BTIS doit fournir des prestations importantes pour que les systèmes d'engagement de l'armée puissent recevoir un appui fiable et durable de la part de l'industrie. Cela nécessite des capacités d'exploitation et de maintenance des systèmes militaires existants et futurs. Parallèlement, des capacités spécifiques sont nécessaires pour que de nouveaux composants puissent être intégrés dans des systèmes militaires, par exemple dans le cadre de mesures de maintien de la valeur. De plus, la BTIS devrait également avoir la capacité de développer et de produire des composants critiques pour la sécurité.

3.3 Personnel de milice

Le système de milice est très important pour l'armée, car il permet un échange de savoirs et de compétences issus des domaines les plus variés. Utilisées à bon escient pendant les cours de répétition ou le service long, les compétences civiles peuvent se révéler bénéfiques pour les deux parties. Cela s'applique aussi aux nouvelles technologies : Grâce au système de milice, il est possible, tant lors du recrutement que pendant le service, de recruter davantage de spécialistes possédant les compétences technologiques et scientifiques nécessaires, de les engager dans leur domaine de compétence et de bénéficier ainsi du bagage civil du personnel de milice. Il importe toutefois que les avantages soient réciproques et que les militaires tirent également profit de leur service pour leur vie civile.

Cyberformation

Grâce à son nouveau stage de cyberformation, l'armée propose deux fois par an une instruction de 40 semaines à une quinzaine de spécialistes informatiques. Les 800 heures qui lui sont consacrées portent sur les domaines suivants : bases générales, bases techniques, instruction transversale (échange de connaissances), instruction à la conduite, instruction spécialisée, ainsi que l'engagement et des exercices. Différentes méthodes d'instruction sont combinées entre elles (p. ex. enseignement frontal, étude personnelle ainsi que l'application et l'approfondissement des connaissances). Les enseignants sont recrutés auprès de la BAC ou à l'externe afin de garantir l'actualité des connaissances et entretenir un lien étroit avec les instituts de formation.

La promotion au grade de sergent prévue dans le cadre du stage permet à ceux qui le suivent d'obtenir un grade plus élevé, ce qui signifie qu'ils sont disponibles plus longtemps pour l'armée avec des connaissances spécifiques. Depuis l'automne 2019, les diplômés du stage peuvent en outre obtenir le brevet fédéral de spécialiste en cybersécurité.

Afin d'améliorer la qualité de l'instruction du stage et de mettre en œuvre des exigences de la *Stratégie nationale de protection de la Suisse contre les cyberrisques*, l'instruction dispensée au sein de l'armée est complétée par un stage réalisé en collaboration avec des partenaires externes. Grâce à cette coopération, les compétences acquises peuvent être approfondies, élargies, et finalement profiter à nouveau à l'armée. Les partenaires pour la réalisation d'un stage sont de préférence les autorités

⁶ Les instruments de pilotage permettant de renforcer la BTIS sont : 1) acquisition en Suisse, 2) affaires compensatoires, 3) coopération internationale, 4) recherche appliquée, 5) promotion de l'innovation, 6) échange d'informations avec l'industrie, 7) politique de contrôle des exportations.

cantonales, les exploitants d'infrastructures critiques et les entreprises suisses actives dans le domaine informatique/cyber. Le concept a été testé une première fois en été 2019. Les entreprises externes proposant un stage dans le cadre d'un projet pilote ont confirmé l'excellence de l'instruction de base et de l'instruction technique. C'est ainsi que l'armée contribue activement à un échange et à l'amélioration de la qualité de la formation dans ce domaine.

Affectation différenciée

Depuis plus de deux ans, l'affectation différenciée permet d'incorporer à la troupe des conscrits ayant des restrictions médicales, par exemple pour porter, soulever des charges ou marcher. Cet aspect sera également pris en considération lors de la révision des directives relatives à l'aptitude au service (règlement *Nosologia Militaris*). En outre, des commissions de visite sanitaire (CVS) spéciales sont compétentes pour évaluer les cas de conscrits et de militaires souffrant de problèmes physiques importants. Ces CVS évaluent au cas par cas l'aptitude à la fonction militaire envisagée et sans préjudice vis-à-vis d'autres cas. Ainsi, lorsque c'est réaliste d'un point de vue médical, les spécialistes peuvent aussi accomplir leur service militaire avec des restrictions médicales. L'objectif premier lors de l'évaluation est toujours de s'assurer que les personnes déclarées aptes au service ne mettent en danger ni leur santé ni celle de leurs camarades en effectuant les services prévus.

Alimentation

La solution la plus durable pour conserver plus longtemps des savoir-faire spécifiques au sein de l'armée est la promotion, qui augmente le nombre maximal de jours de service à accomplir. Ainsi, afin d'augmenter par exemple la durée des obligations militaires des spécialistes de l'industrie, la possibilité existe de promouvoir ces derniers au rang d'officier spécialiste⁷ (Ils devront ensuite effectuer 240 jours de service au maximum après leur nomination, indépendamment des jours de service accomplis jusqu'alors). De plus, il est possible de nommer un militaire, quel que soit son grade initial, à un poste de spécialiste pour une fonction donnée et pour laquelle il effectue également des jours de service supplémentaires. Selon les besoins, et à la demande conjointe de la personne concernée et du commandement responsable, l'armée peut également prolonger l'obligation de servir des sous-officiers supérieurs et des officiers supérieurs afin de pouvoir compter plus longtemps sur leurs connaissances.

Le cadre légal est donné par l'art. 42 de la loi du 3 février 1995 sur l'armée (LAAM)⁸ et l'art. 47 de l'ordonnance du 22 novembre 2017 sur les obligations militaires (OMi)⁹. Celui-ci établit le nombre total de jours de service imputables aux militaires de milice. Ainsi, après que ces derniers ont accompli ce nombre de jours, l'armée ne peut plus bénéficier de leurs connaissances. La révision en cours de la LAAM prévoit de prolonger la durée maximale d'engagement des militaires en service long de 280 à 300 jours de service d'instruction.

En ce qui concerne l'alimentation en effectifs, les profils d'exigences des fonctions de recrutement pour l'affectation initiale des conscrits ont été vérifiés, harmonisés et, le cas échéant, adaptés au 1^{er} juillet 2019. Il est désormais aussi possible de se spécialiser au sein d'une fonction pendant l'instruction. Ainsi, les talents ayant des compétences particulières dans le domaine des nouvelles technologies peuvent être approchés avant leur formation spécialisée et recrutés pour la fonction militaire appropriée. À cela s'ajoute la possibilité de changer l'incorporation de militaires possédant les formations civiles

⁷ En vertu de l'art. 80 OMi (RS 512.21), les fonctions d'officier dans lesquelles les connaissances et les compétences particulières nécessaires sont de première importance peuvent être confiées à des officiers spécialisés.

⁸ RS 510.10

⁹ RS 512.21

correspondantes pour les engager dans une fonction ou une formation appropriée. Les candidats potentiels pour des fonctions spécifiques aux technologies de l'information sont recherchés de manière proactive, mais ceux-ci peuvent aussi répondre volontairement aux offres de l'armée.

Afin que les connaissances particulières des militaires puissent être utilisées pendant une période plus longue, différents modèles sont à l'étude. Une solution envisageable serait de comptabiliser (partiellement) des travaux de master ou de doctorat. Ce modèle est déjà appliqué pour les spécialistes et les candidats aux fonctions de médecin, de dentiste ou de pharmacien. Pour l'instruction des officiers aspirant à ces fonctions hautement spécialisées, le service peut se faire en uniforme sous un commandement militaire, entièrement ou partiellement dans des instituts civils spécialisés, dans le cas où l'armée ne peut assurer elle-même l'instruction. La participation à des formations civiles imputables requiert toutefois que les militaires concernés consentent à rester plus longtemps à disposition de l'armée.

Le Plan d'action Cyberdéfense DDPS prévoit une augmentation substantielle des effectifs, aussi de milice, dans le domaine Cyber. Il est prévu de créer un bataillon cyber et un état-major spécialisé dans ce domaine au 1^{er} janvier 2022, ce qui fera passer les effectifs de milice de 200 environ actuellement à 575 militaires. L'augmentation des effectifs de milice doit permettre avant tout d'améliorer la capacité à durer des moyens opérationnels de l'armée dans ce domaine. À cette fin, les cyberspécialistes de milice seront incorporés dans les formations correspondantes de l'armée.

3.4 Personnel professionnel (civil et militaire)

Compte tenu de la situation sur le marché du travail, le recrutement de spécialistes militaires ou civils constitue un défi. Le marketing du personnel a certes été intensifié, par exemple en étudiant de nouveaux modes de recrutement, en utilisant plus activement les médias sociaux ou en proposant des emplois à temps partiel durant la formation tertiaire. Il faudra cependant un certain temps avant que ces mesures déploient leurs effets. C'est pourquoi il n'est pas encore possible d'évaluer leur impact sur les effectifs.

En plus du recrutement de personnes dotées d'un savoir-faire spécifique sur le marché du travail, il convient de promouvoir l'acquisition et le développement des compétences des collaborateurs. À cet effet, le DDPS veille constamment à ce que le développement du personnel, des cadres et des carrières soient harmonisés et étendus si nécessaire. Les collaborateurs peuvent par exemple suivre des cours du Centre de formation de l'administration fédérale ou conclure des conventions de formation individuelles s'ils accomplissent une formation auprès d'un institut externe à la Confédération.

Outre l'augmentation des effectifs de milice, le Plan d'action Cyberdéfense DDPS prévoit ces prochaines années d'augmenter de moitié environ le nombre de professionnels dans le domaine Cyber. Les collaborateurs de l'administration militaire sont attribués dans le cadre de leurs fonctions aux différents services de la BAC.

ICT Warrior Academy

L'*ICT Warrior Academy* de la BAC est le centre de compétences pour la formation et le perfectionnement du personnel civil du Groupement Défense dans les domaines de l'informatique et des télécommunications. Ce centre propose des formations théoriques et pratiques concernant des fonctions, méthodes et technologies particulières. L'enseignement est dispensé avec le concours d'universités, de hautes écoles spécialisées et de partenaires, et comprend des thèmes comme le *Design Thinking*, la gestion des services informatiques, l'ingénierie logicielle et la cybersécurité. L'*ICT*

Warrior Academy s'adresse à tous les collaborateurs, nouveaux ou anciens, qui doivent être formés spécifiquement pour leur fonction à la BAC.

Le nouveau programme *ICT Warrior School* est ainsi consacré aux prestations, compétences et infrastructures informatiques pour les cinq à dix prochaines années. Il évalue et forme les professionnels en fonction de leurs activités actuelles et leur potentiel, puis les réalloue selon leurs aptitudes et leurs aspirations.

4 Collaboration avec les partenaires

Le DDPS entend collaborer plus étroitement avec l'administration fédérale. Il entretient des partenariats avec des instituts de formation et travaille directement avec des partenaires industriels par le truchement d'armasuisse. Compte tenu de l'évolution technologique, le DDPS vise en tout temps à approfondir les coopérations existantes ou à en établir de nouvelles.

4.1 Instituts de formation

Des accords de coopération existent entre le Groupement Défense et différents instituts de formation, afin que les formations puissent être mutuellement reconnues. Des conventions réglant la prise en considération de l'instruction militaire dans les cours, les stages, la formation initiale, les études consécutives et les formations de perfectionnement ont ainsi été conclues avec une multitude d'instituts de formation tertiaires. Un militaire peut par exemple faire valider des crédits ECTS dans certaines hautes écoles s'il a achevé une formation à la conduite auprès de la Formation supérieure des cadres de l'armée. Il existe en outre des conventions de formation dans le domaine des sciences naturelles et techniques, par exemple avec l'Université de Zurich, l'École polytechnique fédérale de Zurich (EPFZ) et la Haute école de Lucerne.

Campus cyberdéfense du DDPS

Le CYD-Campus est un centre de cybercompétences créé par le DDPS sous la direction d'armasuisse. Il encourage la recherche en matière d'innovation et la recherche appliquée dans les sciences de la sécurité et des données et entend mettre en œuvre les résultats obtenus aux côtés de start-up et d'entreprises spécialisées dans la sécurité. Il sert notamment à identifier les technologies et les cyber tendances et à en évaluer l'utilité. Le savoir requis est développé en collaboration avec des universités et l'industrie, avec le soutien des trois sites du CYD-Campus à Thoun (armasuisse), à l'EPFZ et à l'École polytechnique fédérale de Lausanne (EPFL). Le but premier du campus est de créer des prototypes et des démonstrateurs à partir des résultats de la recherche fondamentale et de développer des partenariats.

Cyber-Defence Fellowships

En 2020, le CYD-Campus et l'EPFL ont lancé conjointement le programme suisse de promotion des talents *Cyber-Defence*. Son but est de développer la recherche et l'enseignement dans le domaine de la cyberdéfense en réunissant la recherche universitaire et la recherche appliquée. Il s'agira de développer des solutions en matière de sécurité des réseaux et de science des données et de mener une réflexion sur des questions technologiques et scientifiques qui vont au-delà de ces thèmes.

Des projets de recherche au niveau du master, du doctorat et du post-doctorat sont proposés deux fois par an dans le cadre du *Cyber-Defence Fellowships*. Le programme *Fellowship* (enveloppe financière d'un million de francs par an environ) permet à des étudiants, des doctorants et des post-doctorants de

mener leurs travaux ou leurs projets de recherche au CYD-Campus sous la supervision d'un professeur d'une haute école suisse. Ce programme ne vise pas seulement à trouver des solutions technologiques ou techniques dans le domaine de la cyberdéfense, mais aussi à créer une nouvelle génération d'experts dans ce domaine.

Encadrement des travaux scientifiques et des stages

Dans le cadre de programmes de recherche, armasuisse confie des travaux scientifiques à des universités et à des hautes écoles spécialisées suisses et les supervise. Concrètement, à l'heure actuelle, une cinquantaine de travaux de bachelor, master, doctorat et post-doctorat couvrent un large éventail de questions technologiques pertinentes pour l'armée. Leurs coûts s'élèvent à quelque cinq millions de francs par an.

Des travaux scientifiques de ce genre peuvent également être menés au Centre suisse des drones et de la robotique d'armasuisse (avec l'EPFZ). Dans un avenir proche, une attention tout particulière sera aussi accordée au thème de l'espace. Les étudiants sont ainsi familiarisés à un stade précoce aux questions technologiques pertinentes pour l'armée, ce qui éveille leur intérêt pour les sujets concernés. Les expériences faites par les étudiants dans ce contexte peuvent faciliter leur entrée à l'armée ou dans les domaines technologiques du DDPS.

Suivant l'université ou la haute école spécialisée concernée, les étudiants peuvent en outre effectuer un stage de trois à douze mois auprès d'armasuisse. Celle-ci propose également des places de stage individuelles, notamment pour aider les étudiants à choisir leur orientation universitaire. Ces stages permettent à armasuisse de déceler rapidement les profils prometteurs et de se positionner en tant que futur employeur.

4.2 Économie privée

La collaboration avec l'économie privée en Suisse et à l'étranger est décrite dans les *Principes du Conseil fédéral en matière de politique d'armement du DDPS*, tout comme l'importance préalablement mentionnée de la BTIS et le rôle de RUAG. Au moment de la dissociation des activités de RUAG Holding SA, les unités opérationnelles consacrées à l'armée ont été séparées du reste du groupe pour devenir une filiale. Celle-ci ne fournit en principe des prestations que pour les systèmes de l'armée. Elle sera le centre de compétences du matériel pour l'acquisition de systèmes complexes relevant de la sécurité.

La collaboration directe avec l'industrie dans le domaine de l'innovation représente un défi. Le DDPS a introduit des mesures afin d'optimiser les processus d'acquisition, notamment parce que la collaboration avec l'industrie gagne en importance en raison de la rapidité avec laquelle les technologies évoluent.

4.3 Coopération internationale

L'évolution technologique joue un rôle important dans la collaboration du Groupement Défense et d'armasuisse avec d'autres États et des organisations internationales. La coopération internationale sert, entre autres, à développer et à maintenir l'accès aux capacités, au savoir-faire et aux compétences à l'étranger.

L'accent est mis sur la coopération avec les États voisins, les organisations internationales en Europe et avec les leaders technologiques mondiaux. Régulièrement, les défis liés à la transformation numérique sont analysés à l'occasion d'échanges d'expériences et lors d'instructions et d'exercices communs. Les coopérations internationales constituent en outre des plateformes pour des projets de recherche communs. Cela est particulièrement important pour la Suisse, lorsque les compétences ou les infrastructures font défaut dans des domaines spécifiques de recherche.

La participation de la Suisse au *Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, à Tallinn (Estonie), qui approfondit la collaboration internationale dans la recherche et la formation en matière de cyberdéfense et de cybersécurité, est un bon exemple de cette coopération. Grâce à celle-ci, la Suisse accède à un savoir, à des informations et aux différentes activités de recherche et de formation du CCDCOE. Sa participation contribue à la mise en œuvre de la *Stratégie nationale de protection de la Suisse contre les cyberrisques*. Dans le cadre de cette coopération, la Suisse pourra aussi détacher un ou deux spécialistes civils ou militaires à Tallinn.

5 Conclusion

L'évolution technologique et la transformation numérique ont une influence sur le DDPS et l'armée. Diverses mesures ont été lancées ou ont déjà été mises en œuvre pour que l'armée et le Groupement Défense disposent à l'avenir de suffisamment de spécialistes ayant des compétences scientifiques et technologiques.

S'agissant des éléments de milice, outre la promotion au grade d'officier spécialiste et la nomination comme spécialiste dans une fonction donnée, il existe la possibilité de changer leur incorporation lorsqu'ils possèdent une formation civile complémentaire, par exemple dans le domaine informatique, pour les engager dans une fonction ou une formation appropriée. L'affectation différenciée permet par ailleurs de recruter un nombre plus important de conscrits pour les former durant leur service militaire et grâce au stage de cyberformation nouvellement créé, il est possible de s'adresser directement à des militaires disposant d'un savoir informatique spécifique. En outre, l'attractivité de certaines formations militaires est renforcée grâce à leur reconnaissance par des instituts civils de formation.

S'agissant du personnel professionnel, l'accent est mis, outre sur le recrutement, sur la formation et le perfectionnement internes, par exemple à l'*ICT Warrior Academy* de la BAC. De plus, des travaux scientifiques, des stages et des programmes de recherche sont proposés en collaboration avec des universités et des hautes écoles spécialisées. L'objectif est de déceler et de promouvoir les talents à un stade précoce et de faciliter l'accession de ces futurs experts à l'administration militaire.

Pour développer et maintenir un savoir-faire technologique, la collaboration au sein de l'administration fédérale et avec les partenaires suisses et étrangers est encouragée. Des conventions de formation sont ainsi conclues avec des instituts de formation, ou des programmes de promotion des talents comme le *Cyber-Defence Fellowships* sont mis sur pied. Le DDPS a également créé le CYD-Campus sous la direction d'armasuisse, qui met notamment en œuvre les résultats de la recherche aux côtés de start-up et d'entreprises spécialisées dans la sécurité. Il est également fait appel à l'économie privée dans le domaine des technologies liées à la sécurité conformément aux *Principes du Conseil fédéral en matière de politique d'armement du DDPS*. Ces mesures assureront un éventail de connaissances et de compétences aussi large que possible pour l'armée.

Dans l'avenir, la technologie, la collaboration avec des partenaires et le personnel qualifié joueront un rôle encore plus important qu'aujourd'hui. C'est pourquoi le DDPS tient compte et promeut les partenariats existants et la création de nouvelles coopérations, s'engage dans le domaine de la recherche et du développement et s'efforce de garantir sur le long terme le recrutement d'un personnel (notamment de milice) possédant une expertise technologique.