Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confedraziun svizra

armasuisse

Plan de recherche à long terme (PRLT) 2025-2028

Plan directeur de recherche armasuisse avec les axes de recherche et les domaines thématiques prioritaires

Plan de recherche à long terme (PRLT) 2025-2028

Plan directeur de recherche armasuisse avec les axes de recherche et les domaines thématiques prioritaires

Publié par
Office fédéral de l'armement armasuisse
Berne, 2024

Impressum

Éditeur

© Office fédéral de l'armement armasuisse (ar)
Département fédéral de la défense, de la protection de la population et des sports (DDPS)

Publication

Octobre 2024

Auteurs

Dr Corina Beerli (ar), Dr Hansruedi Bircher (ar), Dr Kilian Wasmer (ar)

Groupes d'accompagnement et de travail

Groupe de travail PRLT 2025-2028 :
Dr Corina Beerli (ar), Dr Hansruedi Bircher (ar), Nico Grandjean (V, A Stab), Dr Anita Noli-Kilchenmann (V, A Stab), Dr Kilian Wasmer (ar), Oberstlt Dominik Winter (V, A Stab), Alexander Zagoda (V, A Stab)

Groupe de travail sur le domaine de la politique de paix et de sécurité 2025-2028 :
Dr Corina Beerli (ar), Dr Hansruedi Bircher (ar), Dr Cédric Invernizzi (BABS), Gina Menghini (EDA, AIS), Giorgio Ravioli (BABS), Sylvia Völgyi (EDA, AIS), Christoph Werner (BABS)

Sounding Board :
Daniel Bhend (V, Kdo Ausbildung), Urs Born (V, Kdo Cyber), Dr Daniel Fuhrer (V, A Stab), Michael Hirschi (V, LBA), Dr David Humair (V, Kdo Operationen), Michael Nussli (V, LBA), Oberst Daniel Setz (V, Kdo Ausbildung)

Groupe d'experts pour le suivi scientifique :
Dr Gérôme Bovet (ar, Science des données), Dr Peter Erni (ar, Spatial), Dr Markus Höpflinger (ar, Systèmes mobiles sans pilote), Dr Quentin Ladetto (ar, Prospective technologique), Dr Ulrich Langer (ar, Spatial), Dr Ronny Lorenzo (ar, Effets, protection et sécurité), Dr Christof Schüpbach, (ar, Communication), Dr Matthias Sommer (ar, Simulation), Dr Bernhard Tellenbach (ar, Espace cybernétique), Dr Peter Wellig (ar, Reconnaissance et surveillance)

Conception

Lucas Ballerstedt (ar)

Téléchargement PDF

www.ressortforschung.admin.ch

Contact

armasuisse Science et technologies,
wt@armasuisse.ch

Validité version linguistique

La version allemande fait foi en cas d'incohérence ou de divergence entre la version allemande et toute autre version linguistique de la présente publication.

Préambule

Depuis l'élaboration du dernier plan de recherche, plusieurs événements nous ont ébranlés, dont trois d'une portée particulière : la crise du COVID-19, la guerre en Ukraine et l'escalade du conflit au Proche-Orient. Ces événements ont amené la population et les médias à s'intéresser davantage aux aspects de la politique de sécurité.

La crise du COVID-19 a révélé à quel point notre société et notre économie sont vulnérables. Dans ce contexte, les réseaux sociaux ont été de puissants moteurs de radicalisation et de division de la société. L'économie a été confrontée au revers de la médaille de la division internationale du travail et de sa dépendance à l'égard de l'approvisionnement. La crise du COVID-19 a également démontré qu'en fin de compte, chaque pays mettait en avant ses propres besoins et intérêts. D'un autre côté, la pandémie de COVID-19 constitue un bon exemple de la manière dont la recherche permet de fournir les bases nécessaires à une gestion rapide des crises dans un pays innovant comme la Suisse.

La guerre en Ukraine nous a montré que les conflits modernes sont gérés à tous les niveaux : militaire, politique et économique. Ce conflit met également en évidence l'urbanisation de la guerre, l'attaque ciblée d'infrastructures critiques, le nouveau rôle des acteurs civils dans le domaine de la reconnaissance et de la communication par satellite ainsi que l'importance croissante des armes à longue portée ou encore la défense contre ces dernières, de façon à permettre la protection de la population, des propres forces et des infrastructures critiques. Il est frappant de constater la créativité et la rapidité avec laquelle la partie ukrainienne est capable d'utiliser par moments les technologies civiles à son avantage, que ce soit dans le domaine de la reconnaissance tactique, de la désignation des objectifs ou de la localisation des adversaires. Il est également impressionnant d'observer avec quel esprit d'innovation les Ukrainiens utilisent et développent de nouvelles technologies, comme les drones.

La complexité des conflits modernes représente un grand défi pour le développement des forces de sécurité ainsi que pour la planification, l'acquisition et l'exploitation des moyens d'intervention. Les compétences scientifiques, axées à la fois sur l'environnement technologique civil et militaire, jouent ici un rôle central. L'évolution de la technologie doit être observée et les conséquences qui en résultent doivent être anticipées pour la sécurité de la Suisse et mises en œuvre au profit de l'armée. La recherche est donc un instrument permettant de garantir la capacité d'expertise d'armasuisse dans le domaine des technologies essentielles en matière de sécurité. Elle constitue La base pour soutenir le développement – axé sur les capacités – de l'armée, encourager les innovations basées sur la technologie et soutenir les évaluations de systèmes concernant les acquisitions d'armasuisse. La recherche apporte ainsi une contribution essentielle à la sécurité et à l'indépendance durables de la Suisse.

Le présent plan de recherche à long terme définit les priorités thématiques et la méthode permettant d'atteindre cet objectif pour les années 2025 à 2028.

Dr Urs Loher

Directeur général de l'armement

Table des matières

	Zusammenfassung / *Résumé*	**6/7**
1	**Introduction**	**8**
1.1	**Recherche dans l'administration fédérale**	**8**
1.2	**Vue d'ensemble de la politique de sécurité et de paix**	**8**
1.3	**Recherche en matière de politique de sécurité et de paix**	**9**
2	**Science et recherche au DDPS**	**12**
2.1	**Contexte international**	**12**
2.2	**Contexte de la recherche au DDPS**	**12**
2.3	**Positionnement de la recherche au DDPS**	**14**
2.4	**Principes de mise en œuvre stratégiques**	**16**
2.5	**Mandat légal et bases**	**18**
2.6	**Rétrospective de la période 2021-2024**	**18**
2.7	**Défis et actions requises**	**18**
3	**Axes de recherche et domaines thématiques prioritaires 2025-2028**	**20**
3.1	**Prospective technologique**	**22**
3.1.1	Veille technologique	22
3.1.2	Évaluation de l'impact technologique	23
3.2	**Technologies pour les capacités opérationnelles**	**25**
3.2.1	Effets et protection dans l'espace physique	25
3.2.2	Opérations et protection dans le cyberespace et l'espace électromagnétique	28
3.2.3	Technologies pour garantir la supériorité de l'information	33
3.3	**Intégration de la technologie aux plateformes**	**39**
3.3.1	Autonomie et robotique	39
3.3.2	Technologies spatiales et alternatives	42
3.4	**Thèmes transversaux**	**46**
3.4.1	Approvisionnement énergétique durable et autarcique	46
3.4.2	Simulation et analyse	48
3.4.3	Facteurs humains (human factors)	50
4	**Financement**	**52**
4.1	**Financement 2021-2024**	**52**
4.2	**Financement 2025-2028**	**52**
5	**Acteurs et interfaces**	**53**
5.1	**Description des principaux acteurs**	**53**
5.2	**Interfaces avec d'autres offices fédéraux**	**54**
5.3	**Coopération internationale**	**55**
6	**Organisation et assurance qualité**	**57**
6.1	**Organisation interne**	**57**
6.2	**Assurance qualité**	**57**
6.3	**Diffusion des connaissances**	**58**
	Annexe	**60**
A1	**Répertoire des abréviations**	**60**
A2	**Bases légales et documents stratégiques**	**63**

Zusammenfassung

Die Forschung von armasuisse schafft die Grundlage für ein vertieftes Verständnis derjenigen Technologien, welche für die Sicherheit der Schweiz relevant sind. Durch den Aufbau von technisch-wissenschaftlichen Kompetenzen können die Armee, der Nachrichtendienst des Bundes und das Bundesamt für Cybersicherheit mit fundierten und unabhängigen Expertisen unterstützt werden. Die Erkenntnisse aus der Forschung fliessen sowohl in die langfristige Streitkräfteentwicklung als auch in die Evaluation von Systemen während der Beschaffung durch die armasuisse ein. Ferner bildet ein gutes technisch-wissenschaftliches Expertenwissen auch eine gute Basis für technologiegetriebene Innovationen in der Armee und im VBS.

Im vorliegenden Forschungskonzept, dem Langfristigen Forschungsplan (LFP), werden im Rahmen der Ressortforschung des Bundes die inhaltlichen Forschungsprioritäten für den Zeitraum 2025 - 2028 aufgezeigt. Diese orientieren sich an den festgestellten technologischen Megatrends und am Bedarf der sicherheitspolitischen Akteure des VBS, insbesondere der Armee. Die Forschung von armasuisse verfolgt deshalb einen mittel- bis langfristigen Zeithorizont, ist anwendungsorientiert und konzentriert sich auf einen mittleren Technologiereifegrad bis hin zur Realisierung von Demonstratoren. Dabei werden sowohl Kooperationen im Expertennetzwerk als auch multidisziplinäre Ansätze mit potenziellen Nutzern verfolgt.

Dazu wurden vier aufeinander abgestimmte Forschungsschwerpunkte definiert und sind in Abbildung 1 dargestellt:

- Die Technologiefrüherkennung um disruptive Technologieentwicklungen zu erkennen und deren Konsequenzen im sicherheitspolitischen Kontext abzuschätzen. Die Technologiefrüherkennung dient neben der Reduktion von Planungsrisiken von Sicherheitskräften auch der Identifikation von neuen Forschungsthemen.
- Der Forschungsschwerpunkt «Technologien für operationelle Fähigkeiten» zeigt auf ausgewählten Gebieten den Einfluss der Technologieentwicklung auf die operationellen Fähigkeiten von Sicherheitskräften auf. Dabei werden primär die Auswirkungen der Digitalisierung im Rahmen des Sensor-Nachrichtendienst-Führungs-Wirkungsverbund (SNFW), aber auch Wirk- und Schutzprinzipien untersucht.
- Die Integration von Technologien zu Plattformen ist ein Forschungsschwerpunkt, welcher anhand von Demonstratoren das Technologiepotenzial für Einsätze aufzeigen soll. Damit wird auch die Brücke in technologiegetriebene Innovationen von Plattformen geschlagen.
- Die Querschnittsthemen umfassen Forschungsaspekte, welche für eine gesamtheitliche Betrachtung der anderen Forschungsschwerpunkte relevant sind.

Illustration 1: Forschungsschwerpunkte und prioritäre Themenfelder des LFP 2025-2028

Résumé

La recherche d'armasuisse pose les bases d'une compréhension approfondie des technologies qui sont essentielles à la sécurité de la Suisse. Le développement de compétences technico-scientifiques permet de soutenir l'armée, le Service de renseignement de la Confédération et l'Office fédéral de la cybersécurité en leur fournissant des expertises approfondies et indépendantes. Les connaissances issues de la recherche sont intégrées aussi bien dans le développement à long terme des forces armées que dans l'évaluation des systèmes pendant leur acquisition par armasuisse. En outre, une bonne expertise technico-scientifique constitue également une bonne base pour les innovations technologiques au sein de l'armée et au DDPS.

Le présent plan directeur de recherche, à savoir le plan de recherche à long terme (PRLT), met en évidence les axes de recherche en termes de contenus pour la période 2025 - 2028 dans le cadre de la recherche de l'administration fédérale. Ces axes de recherche s'inspirent des mégatendances technologiques constatées et des besoins des acteurs de la politique de sécurité du DDPS, et plus particulièrement de l'armée. C'est pourquoi la recherche d'armasuisse s'inscrit dans un horizon temporel à moyen ou long terme en étant orientée vers les applications et en se concentrant sur un degré de maturité technologique moyen allant jusqu'à la réalisation de démonstrateurs. Cette démarche vise des coopérations au sein du réseau d'experts et des approches multidisciplinaires avec des utilisateurs potentiels.

À cet effet, quatre axes de recherche coordonnés entre eux ont été définis et sont représentés sur l'Illustration 1.

- *La prospective technologique permet d'identifier les développements technologiques disruptifs et d'évaluer leurs conséquences dans le contexte de la politique de sécurité. La prospective technologique sert non seulement à réduire les risques de planification des forces de sécurité, mais aussi à identifier de nouveaux thèmes de recherche.*
- *L'axe de recherche « Technologies pour les capacités opérationnelles » montre, dans des domaines sélectionnés, l'influence de l'évolution technologique sur les capacités opérationnelles des forces de sécurité. Il s'agit en premier lieu d'étudier les effets de la numérisation dans le cadre du réseau intégré de capteurs, de renseignement, de conduite et d'action (CRCA), mais aussi les principes d'action et de protection.*
- *L'intégration des technologies aux plateformes est un axe de recherche censé démontrer, au moyen de démonstrateurs, le potentiel technologique pour les engagements. Cela permet également de faire le lien avec les innovations technologiques des plateformes.*
- *Les thèmes transversaux englobent des aspects de la recherche qui sont pertinents pour une approche globale des autres axes de recherche.*

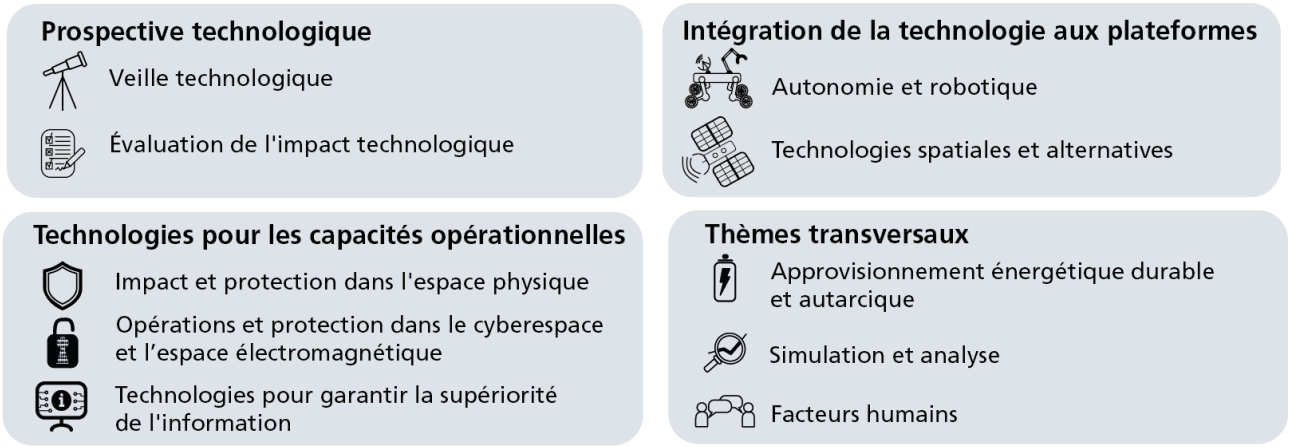


Illustration 1: Axes de recherche et domaines thématiques prioritaires du PRLT 2025-2028

1 Introduction

1.1 Recherche dans l'administration fédérale

L'administration fédérale initie et soutient la recherche scientifique dont les résultats lui sont nécessaires pour accomplir ses tâches. Cette recherche effectuée dans l'intérêt public est appelée recherche de l'administration fédérale. Elle comprend des bases scientifiques pour le développement et l'élaboration de politiques dans différents domaines d'actions, pour les travaux d'exécution dans le cadre des prescriptions légales, pour les travaux législatifs ou pour répondre à des interventions parlementaires et les mettre en œuvre. La recherche de l'administration fédérale peut englober pratiquement toutes les formes de recherche scientifique, allant notamment de la recherche fondamentale jusqu'au développement d'installations pilotes et de démonstration, en passant par la recherche orientée vers les applications. La recherche de l'administration fédérale s'appuie sur des bases légales claires. Elle s'appuie sur l'art. 64 de la Constitution fédérale (RS 101) et sur sa loi-cadre, à savoir la loi sur l'encouragement de la recherche et de l'innovation (LERI, RS 420.1). La responsabilité principale de la recherche de l'administration fédérale incombe aux différents départements et services fédéraux. La coordination générale de la recherche de l'administration fédérale est assurée par un comité de coordination interdépartemental permanent. Dans l'optique de la période FRI 2025-2028, un document commun des services fédéraux a été élaboré, présentant une vue d'ensemble de la recherche de l'administration fédérale ainsi que des défis fondamentaux à venir et des principaux champs d'action. Les programmes pluriannuels sont élaborés pour chacun des onze domaines politiques déterminés par le Conseil fédéral, et ce sous la forme de plans directeurs de recherche interdépartementaux. Dans ce contexte, la recherche d'armasuisse relève du domaine de la politique de sécurité et de paix.

1.2 Vue d'ensemble de la politique de sécurité et de paix

Bases et objectifs de la politique suisse de sécurité et de paix

Conformément à la Constitution fédérale, la Confédération suisse protège la liberté et les droits du peuple et préserve l'indépendance et la sécurité du pays. La Confédération suisse s'engage en outre pour la prospérité du pays, contribue à soulager la misère et la pauvreté dans le monde et promeut le respect des droits de l'homme et de la démocratie pour une coexistence pacifique des peuples. Le domaine de la politique de sécurité et de paix comprend, dans le cadre de la recherche de l'administration fédérale, le soutien à la mise en œuvre politique des aspects de la sécurité et de la paix de la Suisse. Pour garantir ces mandats constitutionnels, la Suisse adopte une approche intégrée et inclusive de la politique de sécurité et de paix.

Dans le cadre de la politique de sécurité, l'objectif est de garantir la capacité d'agir, l'autodétermination et l'intégrité de la Suisse et de sa population, de protéger ses ressources vitales contre les menaces et les dangers directs et indirects et de contribuer à la stabilité et à la paix au-delà des frontières nationales. Afin de poursuivre les objectifs en matière de politique de sécurité, la Suisse dispose de différents domaines politiques et instruments qui sont utilisés de manière coordonnée. Concernant les domaines politiques, il s'agit de politique étrangère et de politique économique ; concernant les instruments, il s'agit de l'armée, de la protection de la population, du service de renseignement, de la police, de l'administration des douanes et du service civil.

L'objectif de la politique de paix est de prévenir, de désamorcer ou de résoudre les conflits violents, de renforcer les droits de l'homme et d'encourager les processus démocratiques. Cela se fait par la voie politico-diplomatique et opérationnelle, grâce à l'instauration de la confiance, à la médiation et aux activités de promotion de la paix après la fin de conflits violents. En outre, le droit international humanitaire est promu et les droits politiques, économiques, sociaux et culturels des personnes ou de groupes de personnes sont renforcés.

Situation en matière de politique de sécurité et conséquences sur la politique de sécurité et de paix

Ces dernières années, l'environnement de la politique de sécurité et de paix en Suisse a fondamentalement changé. Il est placé sous le signe d'une concurrence croissante entre les grandes puissances et de l'action des États menée dans leur propre intérêt. La remise en question des normes internationales et les nombreuses crises ont un impact direct sur la sécurité de la Suisse, que ce soit à moyen ou à long terme. La capacité d'action des organisations internationales de sécurité, comme l'ONU ou de l'OSCE, est en recul. Les défis

à relever dans les domaines de la sécurité, de l'environnement ou de la santé requièrent une réaction coordonnée, qui va au-delà de l'action d'un seul pays. La Suisse a donc tout intérêt à s'engager pour le renforcement et le maintien des règles du droit international public et des droits de l'homme. La population suisse apporte toujours un soutien massif à l'engagement international et humanitaire de la Suisse.

Les conséquences de cette situation pour la population suisse sont le résultat de différentes évolutions interdépendantes qui se renforcent parfois. Comme le montre la guerre en Ukraine, un conflit armé avec son lot de conséquences sur l'Europe et la Suisse peut avoir, assez rapidement, des répercussions à différents niveaux (approvisionnement, économie, migration et diplomatie p. ex.). Dans ce genre de conflit, les droits de l'homme et les principes de l'état de droit sont continuellement violés. La diplomatie suisse s'engage pour une solution pacifique de la guerre, même si la conception suisse de la neutralité est également mise à rude épreuve. La diffusion rapide des technologies modernes accroît le risque d'utilisation abusive de technologies telles que celle des drones, de l'intelligence artificielle et des cyberarmes, ainsi que le risque de transfert d'armes de destruction massive. On constate en outre que les menaces d'utilisation d'armes atomiques se multiplient, que des accusations sont portées au sujet de programmes d'armes biologiques et que des États mènent contre leurs opposants des opérations utilisant des agents NBC. La polarisation de la société constitue un terreau fertile pour l'extrémisme violent et le terrorisme. On constate en outre une augmentation des catastrophes environnementales liées au climat, qui débouchent souvent sur des crises, voire des conflits armés. Il s'agit là d'une cause de l'augmentation des mouvements migratoires qui continueront à solliciter l'aide humanitaire de la Suisse à l'avenir.

1.3 Recherche en matière de politique de sécurité et de paix

Coordination dans le cadre de la recherche de l'administration fédérale

ILes activités de recherche dans le domaine de la politique de sécurité et de paix sont coordonnées et harmonisées dans le cadre de la recherche de l'administration fédérale. L'Office fédéral de la protection de la population (OFPP) et l'Office fédéral de l'armement (armasuisse) du DDPS ainsi que les divisions Sécurité internationale (DSI) et Paix et droits de l'homme (DPDH) du Département fédéral des affaires étrangères (DFAE) y participent.

Les présents plans directeurs de recherche d'armasuisse et de l'OFPP fixent des orientations stratégiques et définissent des axes de recherche et des domaines thématiques harmonisés pendant une période de quatre ans. Même pendant cette période d'application, l'évolution du contexte est toujours prise en compte afin de pouvoir éventuellement adapter l'orientation. L'orientation des activités dans le cadre de la recherche de l'administration fédérale est censée aider à comprendre et à anticiper l'évolution dans cet environnement. Cela permet de garantir, d'une part, la mise à disposition de compétences scientifiques en temps voulu, en tant que base pour une gestion adéquate des tâches dans le futur environnement de la politique de sécurité et de paix et, d'autre part, le conseil interne aux politiques et à l'administration.

Les objectifs de la politique suisse de sécurité et de paix ne peuvent être atteints qu'en adaptant soigneusement les instruments aux menaces actuelles et prévisibles. Compte tenu de la volatilité de la situation en matière de politique de sécurité et de l'imbrication des menaces et des dangers, il convient d'assurer la coopération entre les acteurs majeurs en matière de politique de sécurité et de paix. Pour ce faire, il est nécessaire de maîtriser une grande complexité. Une orientation efficace des différents instruments ne peut aboutir que si une approche flexible est adoptée. Il est essentiel que les domaines de compétence des différents acteurs de la politique de sécurité soient clairement définis et coordonnés entre eux. À cet effet, il est nécessaire d'avoir des connaissances approfondies sur les interfaces et les effets réalisables dans le contexte de l'environnement respectif. Dans le cadre de la politique de sécurité et de paix, la recherche de l'administration fédérale permet non seulement d'assurer la coordination des activités de recherche sur le plan fédéral, mais aussi de mandater le Center for Security Studies (CSS) de l'École polytechnique fédérale de Zurich (EPFZ). Le CSS se concentre en premier lieu sur la recherche dans des domaines des sciences sociales tels que les sciences politiques, l'histoire, le management, la conduite et l'économie. La coordination et la collaboration quant au contenu sont assurées par le comité consultatif DDPS-CSS, auquel participent le Secrétariat général du DDPS, l'Académie militaire (ACAMIL), l'OFPP, armasuisse et le CSS, et par le comité consultatif DFAE-CSS, auquel participent la DSI, la DPDH, la

division Policy Planning (planification politique) et la division Numérisation (Division for Digitalisation).

Alors que le DFAE concentre ses recherches sur la promotion internationale de la paix, la médiation et la facilitation, l'OFPP se focalise sur la maîtrise des armements, la protection des infrastructures critiques et la promotion de la résilience de la société en cas d'événements nucléaires, biologiques et chimiques. armasuisse met d'une part en évidence les conséquences des développements technologiques sur le paysage sécuritaire de la Suisse et soutient d'autre part, grâce à la recherche, le développement des compétences technico-scientifiques de la planification militaire globale et du processus d'armement.

Champs d'action communs de la politique de sécurité et de paix

Dans le contexte des développements actuels en matière de politique de sécurité et de paix, quatre champs d'action et de recherche sont pertinents dans la recherche commune de l'administration fédérale (Illustration 2).

Durabilité
Dans le contexte de la politique de sécurité, la notion de durabilité est comprise au sens très large. Le changement climatique, la situation politique mondiale et les conflits en cours incitent à repenser les méthodes utilisées jusqu'à présent pour garantir la sécurité et la paix. Ainsi, le changement climatique provoque des phénomènes météorologiques extrêmes et favorise de ce fait la pénurie de ressources, la pauvreté, les conflits et les migrations dans les pays émergents et en voie de développement. En mettant en œuvre une politique de paix globale et inclusive, la Suisse tente de promouvoir sur place des structures démocratiques et d'État de droit. Au niveau national, les effets du changement climatique se traduisent par un risque accru de dangers naturels, par des périodes de sécheresse et par une perte de la biodiversité. C'est pourquoi les objectifs climatiques de la Confédération doivent également être mis en œuvre pour les instruments de la politique de sécurité et de paix. Il convient en outre d'assurer une gestion durable des ressources. Pour la Suisse, petit État neutre, il est essentiel de promouvoir les organisations internationales et donc un ordre mondial fondé sur des règles pour contrebalancer les politiques d'hégémonie de plus en plus fréquentes. La guerre en Ukraine a montré que la Suisse doit se préparer aux multiples conséquences de tels conflits et que les instruments de la politique de sécurité, et notamment l'armée, doivent être préparés pour les cas de défense.

Nouvelles technologies
Les progrès technologiques de la dernière décennie ont été énormes et aucun ralentissement n'est à prévoir à ce niveau. Les modèles d'affaires traditionnels ont été supplantés et de nouveaux grands groupes internationaux ont pris une place dominante sur le marché. Du fait de leur orientation vers des marchés potentiels aussi grands que possible, les technologies modernes sont largement disponibles, même si l'on constate qu'une sphère économique d'influence américaine et une sphère économique d'influence chinoise semblent s'établir. Leur impact sur la société est également évident. Dans le cadre de la politique de sécurité et de paix, il convient d'accorder une attention accrue, d'une part, aux conséquences des progrès technologiques interdisciplinaires et de plus en plus complexes et, d'autre part, à la convergence des disciplines. Pour pouvoir faire face de manière fondée à la menace de la prolifération, au risque d'abus et à l'utilisation par des acteurs adverses, il est nécessaire de comprendre fondamentalement l'évolution technologique et ses conséquences pour une intervention de l'État. Cela concerne par exemple les armes chimiques, biologiques et nucléaires, les systèmes autonomes, l'intelligence artificielle et les progrès dans l'utilisation de l'espace exoatmosphérique.

Résilience
Pour faire face aux crises internationales à l'avenir, la Suisse doit renforcer sa capacité d'anticipation et de résilience. L'objectif est de réduire les dépendances face à la volatilité des chaînes de distribution internationales et de renforcer la sécurité d'approvisionnement des biens critiques, des biens d'importance vitale et des biens essentiels en matière de sécurité. Il s'agit notamment de l'approvisionnement en énergie, du système de santé ainsi que des compétences technologiques et des capacités industrielles essentielles en matière de sécurité, qui contribuent à la souveraineté technologique de la Suisse. Il s'agit également d'améliorer la protection et la capacité de régénération en cas de catastrophes et de situations d'urgence. Pour cela, il est nécessaire d'anticiper les dangers naturels, les dangers liés à la technique et les dangers liés à la société, de prévenir les événements, de protéger la population et les infrastructures, et de mettre en place des moyens et des structures pour y faire face. En outre, pour prévenir le terrorisme, l'extrémisme violent et le crime organisé, la Suisse doit empêcher l'établis-

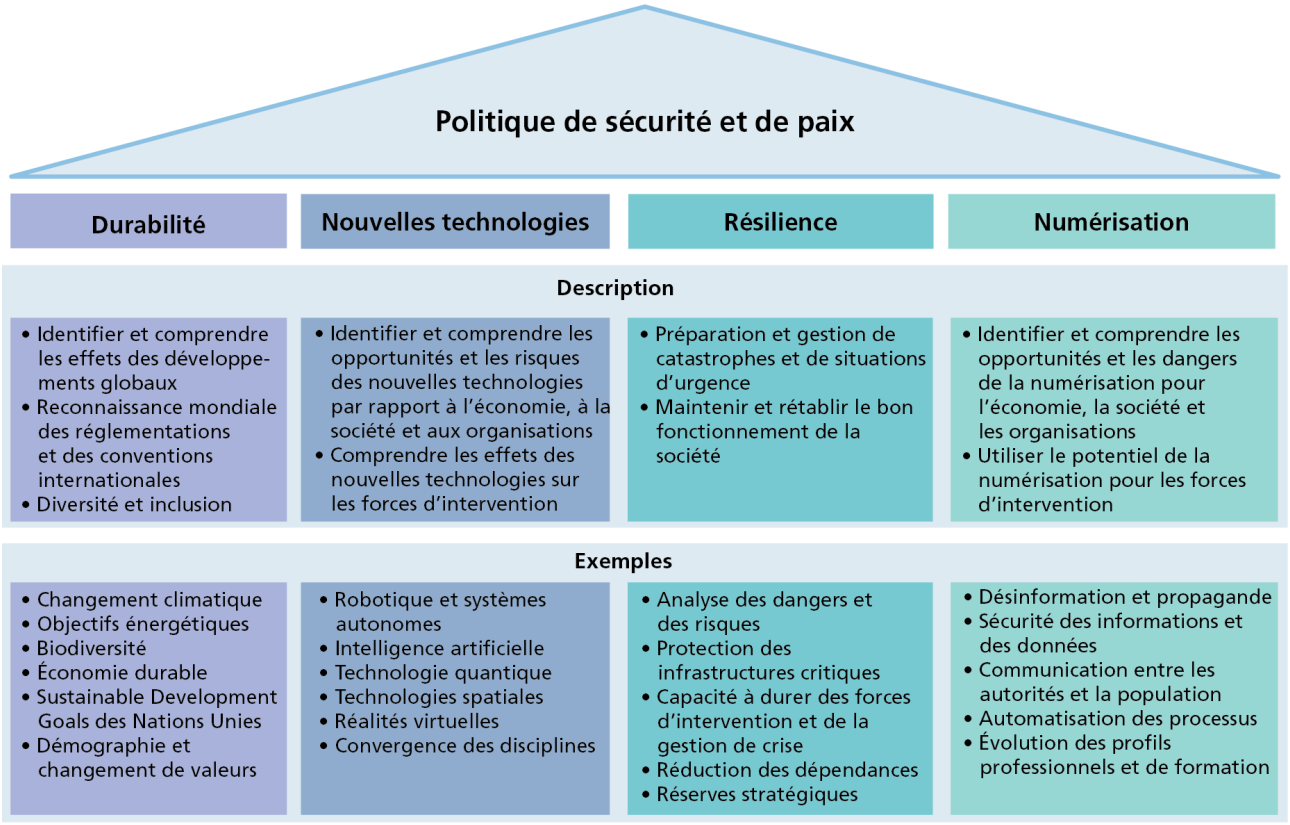


Illustration 2: Champs d'action et de recherche de la politique de sécurité et de paix. Classement des conditions-cadres communes et de leurs effets sur la population, la société et l'économie suisses en matière de politique de sécurité et de paix.

sement des organisations œuvrant à ces fins malveillantes. Pour ce faire, il convient de lutter contre la circulation irrégulière des personnes et des marchandises à la frontière et contre les effets secondaires négatifs de la migration.

Numérisation

Les processus des autorités et des organisations œuvrant dans le cadre de la politique de sécurité sont de plus en plus numérisés pour permettre leur réalisation plus efficace, plus rapide et plus transparente. En outre, les données numériques doivent être exploitées par l'intelligence artificielle afin d'atteindre un degré d'automatisation plus élevé. Les données numériques et l'intelligence artificielle permettent d'utiliser des sources de données ouvertes pour obtenir des informations et, à l'inverse, des données appartenant à la Confédération peuvent être mises à la disposition des utilisateurs. Pour profiter pleinement des opportunités offertes par la numérisation, la Suisse doit continuer à renforcer sa protection contre les cyberrisques. Pour ce faire, elle doit anticiper les évolutions essentielles en matière de sécurité dans le domaine cyber et disposer des moyens nécessaires pour identifier rapidement les cyberincidents et les endiguer grâce à des contre-mesures actives. La libre formation de l'opinion et les informations authentiques constituent la base de tout processus démocratique de formation de l'opinion. La protection de l'État et de ses institutions, de l'économie et de la population contre les cybermenaces, les activités d'influence, l'espionnage et la menace ou l'exercice de la violence doit être assurée. Pour ce faire, il est nécessaire de garantir une communication active basée sur des faits, mais aussi d'identifier la désinformation et la propagande et de prendre des mesures de protection si nécessaire.

2 Science et recherche au DDPS

En Suisse, la mise en œuvre des objectifs de la politique de sécurité passe par une approche inclusive et coordonnée de différents instruments et éléments opérationnels. Le DDPS est responsable de l'armée, de la protection de la population et du service de renseignement. Avec la création de l'Office fédéral de la cybersécurité, un élément supplémentaire est venu s'ajouter. Alors que le plan directeur de recherche de l'OFPP s'oriente en premier lieu sur les besoins de la protection de la population, le plan de recherche à long terme (PRLT) d'armasuisse Science et technologies (S+T) se concentre sur les besoins de l'Armée suisse, du service de renseignement, des services d'achat d'armasuisse et de l'Office fédéral de la cybersécurité. La recherche d'armasuisse permet d'assurer les bases scientifiques nécessaires afin de conseiller et de soutenir les services demandeurs.

2.1 Contexte international

D'une manière générale, on observe que le développement de technologies pertinentes pour les forces armées est aujourd'hui souvent impulsé par les marchés civils. Pour de nombreuses entreprises, le délai de mise sur le marché de nouveaux produits est alors un facteur de réussite essentiel, ce qui accélère énormément le rythme des évolutions technologiques. Sur le plan économique et social, la numérisation est déjà bien avancée. Cependant, la plupart des armées sont à la traîne par rapport à cette évolution. Les raisons en sont multiples. D'une part, l'environnement militaire a longtemps manqué d'une culture de l'innovation pour faire progresser la transformation numérique. D'autre part, la focalisation des entreprises technologiques sur les marchés civils a souvent conduit à ce que les exigences militaires nécessaires pour un engagement sûr et robuste n'ont pas été mises en œuvre pour des raisons de coûts et de temps. Ainsi, les technologies destinées à être utilisées dans un contexte militaire ont dû être soumises à des développements ultérieurs coûteux et chronophages. L'influence de l'État sur le développement des technologies militaires crée souvent des oligopoles et des monopoles pour les produits renforcés destinés à un usage militaire, avec tous les inconvénients que cela comporte concernant la disponibilité dans le temps des technologies les plus récentes et leur prix. À l'inverse, le conflit ukrainien a montré que des moyens low-cost issus du monde civil pouvaient être efficacement modifiés et détournés à des fins militaires en un temps record. C'est pourquoi il est nécessaire d'observer le développement de technologies militaires et civiles, d'évaluer leurs possibilités d'application, tant pour les forces armées régulières que pour les unités opérant de manière hybride, et d'identifier ainsi à temps les opportunités et les menaces pour les propres forces armées. Une solide compétence dans les technologies modernes issues de l'environnement civil ouvre un potentiel d'innovation important pour les applications dans le contexte militaire.

Pour la Suisse, en tant que nation disposant d'un budget de recherche relativement faible dans le domaine des technologies essentielles en matière de sécurité, il est inévitable que des lacunes devront être acceptées en toute connaissance de cause. Cela vaut aussi bien pour la diversité des thèmes que pour la profondeur de leur traitement. La comparaison avec les thèmes de recherche d'autres pays occidentaux et le rapprochement avec les compétences demandées dans le cadre du mandat de l'armée et d'armasuisse montrent que l'orientation thématique de la recherche correspond largement aux besoins ainsi qu'aux tendances technologiques internationales connues. L'intégration d'experts dans des réseaux nationaux et internationaux garantit à la fois la qualité du développement des compétences et le transfert de connaissances du réseau vers le DDPS.

2.2 Contexte de la recherche au DDPS

Pour la planification militaire globale, l'Armée suisse suit l'approche d'un développement des forces orienté capacités (DFOC, Illustration 3). Le grand cycle DFOC, qui s'étend sur une législature, permet (en théorie) de concevoir une nouvelle armée ou de revoir en profondeur le modèle d'armée existant. Le grand cycle s'inscrit dans une perspective à moyen et long terme de 8 à 12 ans. Le point de départ est ici l'anticipation qui prend en compte le contexte militaire, technologique, politique et social, y compris les scénarios planifiés. Sur cette base, des réflexions stratégiques militaires sont élaborées, dont la priorisation des capacités opérationnelles ou des domaines de capacités. L'étape suivante consiste à élaborer des bases de référence, notamment des hypothèses sur une menace concrète. Les bases de référence permettent de formuler la doctrine militaire, y compris les capacités opérationnelles (situation visée). La doctrine constitue la base de l'élaboration des concepts d'opérations, c'est-à-dire la manière concrète dont l'armée doit remplir ses missi-

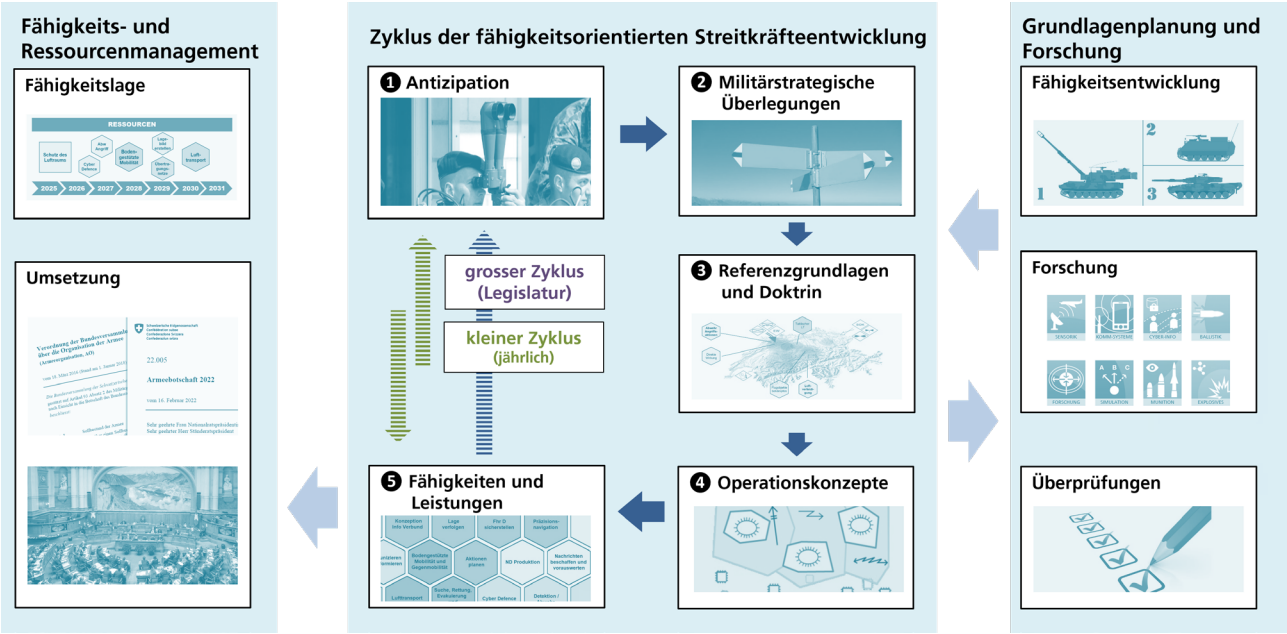


Illustration 3: Processus du développement des forces orienté capacités (DFOC).

ons selon les scénarios planifiés. Nous obtenons ainsi les fondements requis pour décrire les capacités et les performances nécessaires ainsi que la conception de l'armée. Dans le petit cycle DFOC, les produits élaborés pendant le cycle en cours sont examinés chaque année dans l'optique d'une mise à jour, cet examen portant en particulier sur les scénarios planifiés, les capacités et les performances.

Cette approche cyclique est soutenue par des travaux permanents. La gestion des capacités et des ressources comprend, d'une part, l'état des capacités actuel et, d'autre part, la mise en œuvre permanente et l'utilisation des capacités. Dans le cadre de la planification de base et de la recherche, on exploite en quelque sorte un ensemble de réflexions conceptuelles. Ces réflexions peuvent, d'une part, être intégrées dans le cycle et, d'autre part, servir de base à la mise en œuvre et à la gestion des capacités et des ressources. La recherche, l'élaboration des documents de base ainsi que la vérification et l'actualisation des contributions créées sont planifiées respectivement sur plusieurs années. La planification permanente des capacités permet de garantir la disponibilité de bases actuelles en temps voulu, avant que de grands systèmes importants pour les capacités ne soient mis hors service.

En complément de ce processus de planification militaire globale, l'armée a lancé le système d'innovation de la Défense, qui vise la mise en œuvre à court terme d'idées novatrices, en premier lieu pour promouvoir la transformation numérique des forces armées et de l'administration militaire. La recherche d'armasuisse élabore de manière anticipative les bases nécessaires pour pouvoir soutenir aussi bien le processus DFOC que les processus d'innovation de l'armée avec les compétences technico-scientifiques requises.

Cette tâche est assumée par armasuisse conformément à l'ordonnance sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (Org-DDPS). Le domaine de compétences S+T s'y voit attribuer la fonction d'un centre technologique qui couvre les besoins scientifiques et technologiques, et ce également dans le cadre de réseaux et de coopérations avec des partenaires nationaux et internationaux. Selon le règlement d'organisation du DDPS (RO DDPS), l'acquisition des compétences technologiques nécessaires se fait par des activités de recherche appliquée. Les principes du Conseil fédéral pour la politique d'armement du DDPS font également référence à l'instrument de la recherche appliquée, aux coopérations internationales et à l'encouragement de l'innovation, ceci notamment dans le but de renforcer la base technologique et industrielle importante pour la sécurité (BTIS) en Suisse et de garantir des compétences scientifiques et techniques essentielles conformément aux besoins de l'armée. Afin de limiter la dépendance vis-à-vis de l'étranger, il est prévu de développer et d'assurer des compétences dans les technologies prioritaires essentielles en matière de sécurité, telles que les capteurs, les technologies de l'information et de la communication, et ce avec des partenaires suisses dans la mesure du possible.

La collaboration entre les domaines départementaux Défense et armasuisse est réglée au moyen d'une convention de collaboration (CODA). Ce document définit notamment le rôle du responsable de la recherche, qui est chargé aussi bien de l'orientation et de la planification stratégiques que de la mise en œuvre opérationnelle de la recherche au profit d'armasuisse et de l'armée. La CODA, par le biais de la fonction du responsable de la technologie, garantit le transfert de connaissances de la recherche vers la planification militaire globale et les processus d'acquisition. L'objectif est de s'assurer, à un stade précoce de la planification, que les développements technologiques sont pris en compte de manière appropriée dans les projets d'acquisition. Il faut tenir compte du fait que le Centre de compétences pour la médecine militaire et de catastrophe de l'armée fait lui-même de la recherche appliquée afin d'assurer le transfert des connaissances dans la formation, la formation continue et le perfectionnement sur une base scientifiquement fondée. À cet effet, il est prévu de mettre en place un campus virtuel qui, sur la base d'une plateforme numérique de recherche et de connaissances, favorisera la mise en réseau avec la milice et l'environnement universitaire.

Afin de répondre de manière suffisante aux besoins futurs du DDPS en matière d'innovation, armasuisse S+T a été chargé par la cheffe du département de mettre en place des espaces d'innovation. Il s'agit ainsi de créer, pour l'ensemble du DDPS, les conditions organisationnelles, méthodologiques et techniques permettant de promouvoir les innovations portées par la technologie et de créer une culture d'innovation ouverte. Les espaces d'innovation du DDPS soutiennent le système d'innovation de la Défense en mettant à disposition, selon les besoins de l'armée, des compétences technico-scientifiques, le réseau d'experts, des méthodes et des processus pour l'élaboration de solutions innovantes. Les autres partenaires de mise en œuvre pour les projets d'innovation du Groupement Défense sont la RUAG Innovation Organisation et l'unité Swiss Innovation Forces.

2.3 Positionnement de la recherche au DDPS

La recherche d'armasuisse a pour objectif de mettre à disposition les compétences technico-scientifiques nécessaires pour conseiller les décideurs de l'armée sur les questions technologiques, garantir la capacité d'expertise et d'essai tout au long du processus d'armement ainsi que pour mettre en évidence et évaluer suffisamment tôt les développements technologiques et leurs effets sur les capacités opérationnelles de l'armée. Afin de pouvoir évaluer les opportunités et les dangers liés à l'utilisation de nouvelles technologies, il convient de mettre en évidence leur potentiel à l'aide de démonstrateurs et de faire ainsi le lien avec le système d'innovation D et les espaces d'innovation du DDPS. L'objectif est de réduire le temps nécessaire entre la recherche et l'utilisation opérationnelle d'une technologie et de pouvoir ainsi garantir la flexibilité nécessaire des forces d'intervention militaires dans un environnement volatile. Sur la base de ces objectifs, la recherche d'armasuisse s'oriente sur les mégatendances technologiques, la planification militaire globale

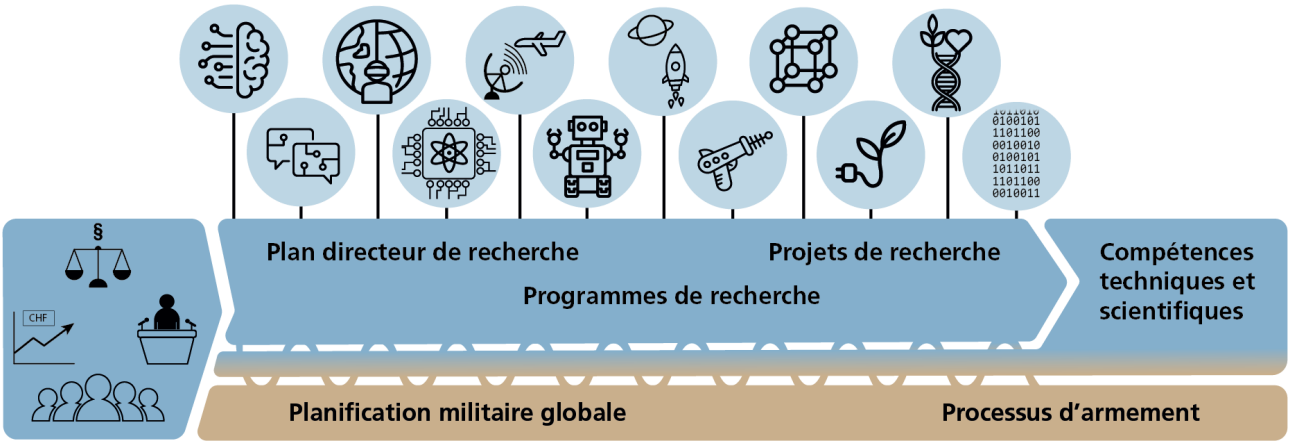


Illustration 4: La recherche d'armasuisse est influencée par différents facteurs. Parmi les facteurs externes, on trouve la politique, l'économie, la société, le droit et les mégatendances technologiques. La planification militaire globale et le processus d'armement influencent l'orientation de la recherche et intègrent également les résultats de la recherche. L'objectif de la recherche est de développer des compétences technico-scientifiques.

et le processus d'armement ainsi que sur des facteurs externes tels que la politique, l'économie, la société et le cadre juridique (Illustration 4).

Afin d'identifier les principales mégatendances technologiques (Illustration 5) pertinentes pour la politique de sécurité de la Suisse, il convient d'observer à grande échelle les développements technologiques menés à l'échelle mondiale et de les évaluer en permanence quant à leur potentiel d'application. Une telle approche permet d'identifier à temps les nouvelles menaces émergentes pour une société et de déduire des mesures pour y faire face, mais aussi de saisir les opportunités pour de futurs scénarios d'intervention. Il convient d'être particulièrement attentif au fait que la combinaison de développements technologiques peut entraîner des effets disruptifs susceptibles de modifier fondamentalement la société, les modèles commerciaux, mais aussi les approches des acteurs dans le contexte de la politique de sécurité. L'identification et l'analyse des mégatendances technologiques constituent donc un instrument permettant de reconnaître de manière précoce les changements induits par la technologie dans l'environnement de la politique de sécurité et de soutenir ainsi le cycle du développement des forces orienté capacités.

Le processus DFOC (développement des forces orienté capacités) constitue également une base importante pour définir les thèmes de recherche d'armasuisse. Sur la base des futurs besoins de capacités de l'armée et de la planification de la mise en œuvre qui en découle, les compétences technologiques nécessaires pour garantir la capacité d'expertise technico-scientifique au profit de l'armée sont développées. Cette capacité s'étend de la collaboration pour la planification de base jusqu'à l'exercice du rôle de responsable de la technologie ou des essais dans les projets d'acquisition. Il s'agit aussi bien de choisir les technologies appropriées pour garantir les capacités opérationnelles que de planifier l'arrêt et le remplacement des technologies en fonction de leur cycle de vie. Pour cela, des compétences technologiques approfondies et une expérience des applications sont nécessaires. Ces deux éléments peuvent être mis en place grâce à la recherche appliquée et à l'innovation.

Dans le paysage de la recherche et de l'innovation (Illustration 6), armasuisse S+T assume une fonction de plaque tournante qui coordonne et regroupe les compétences technologiques au profit de l'armée. Pour ce faire, il est nécessaire de mettre en place un vaste réseau composé de différents acteurs, qu'ils soient issus de l'environnement de la recherche publique et privée mais aussi du milieu des start-up et des entrepreneurs axés sur la technologie. La coordination avec les instruments nationaux d'encouragement de la recherche et de l'innovation permet d'identifier les chevauchements thématiques et de mettre à profit les compétences existantes pour la recherche, mais aussi pour les projets d'innovation du DDPS, selon le principe « add-on ». Enfin, la collaboration avec les institutions de recherche et d'innovation de l'Organisation du Traité de l'Atlantique Nord (OTAN) et de l'Agence Européenne de Défense (AED) aide à élaborer et à échanger des compétences technologiques et des expériences dans le contexte d'un environnement militaire.

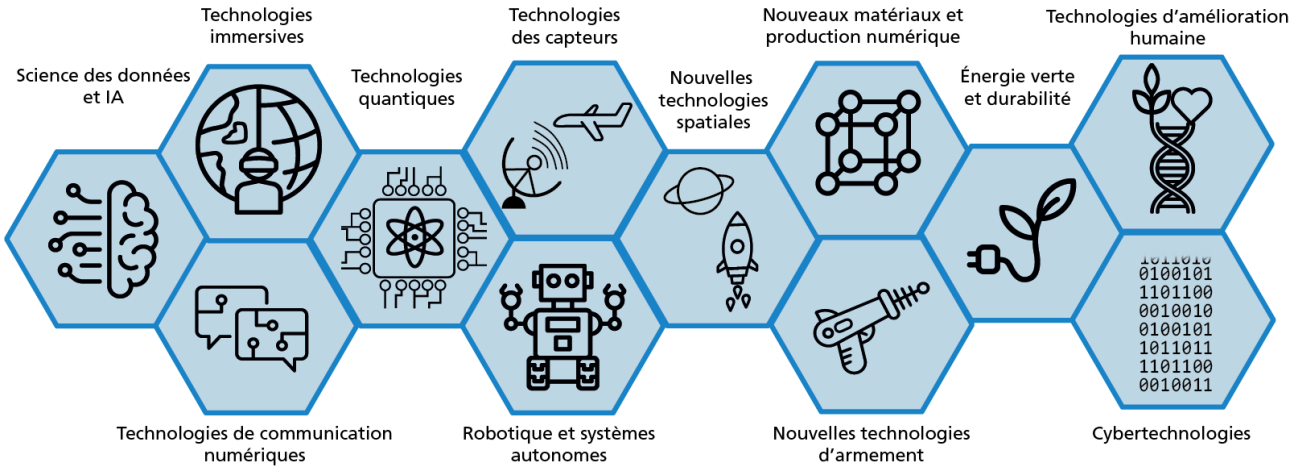


Illustration 5: Mégatendances technologiques identifiées comme importantes pour les forces de sécurité.

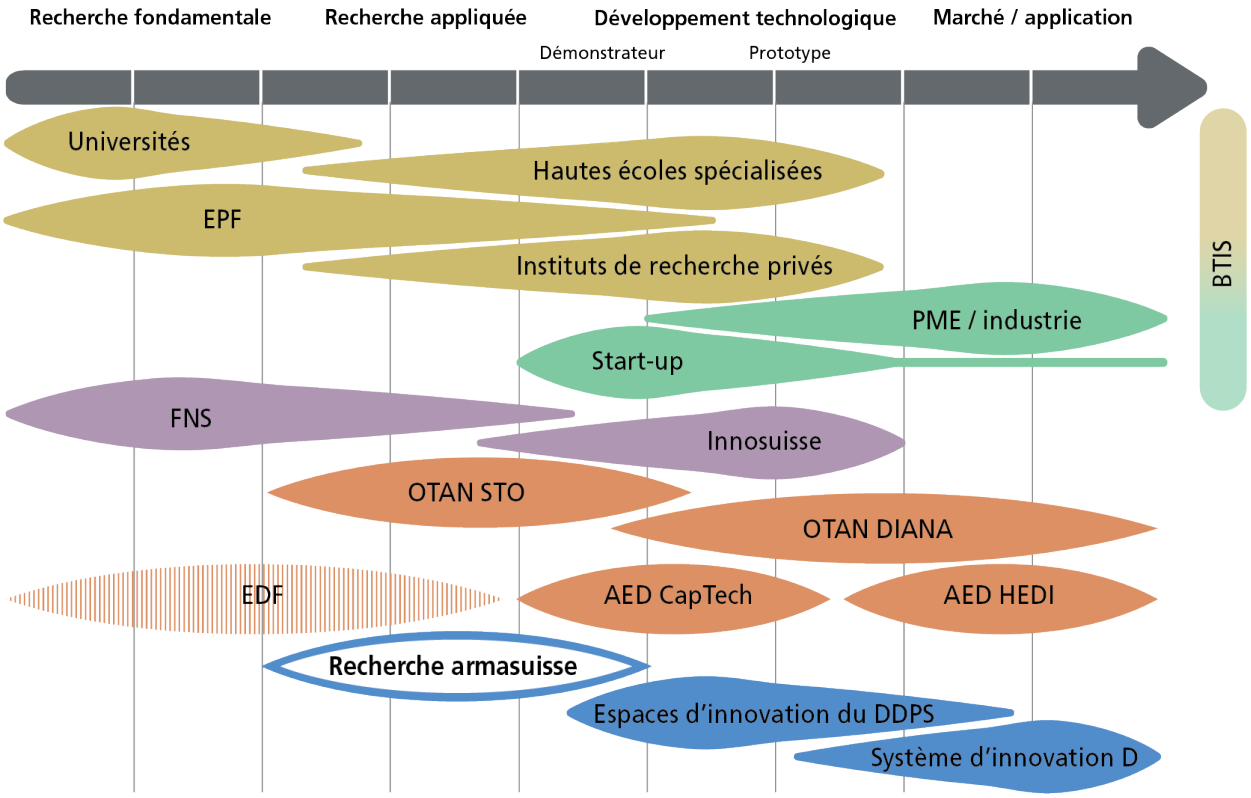


Illustration 6: Classement de la recherche appliquée d'armasuisse dans le paysage de la recherche et de l'innovation du DDPS. Les établissements de recherche et les entreprises qui disposent en Suisse de compétences, d'aptitudes et de capacités dans le secteur des technologies de sécurité et de défense font partie de la base technologique et industrielle importante pour la sécurité (BTIS). Le Fonds national suisse (FNS) dans le domaine de la recherche et Innosuisse dans le domaine de l'innovation sont des instruments d'encouragement importants. Au niveau international, la Suisse peut participer à des projets de l'Organisation pour la science et la technologie (Science and Technology Organization, STO) de l'OTAN et de l'Accélérateur d'innovation de défense pour l'Atlantique Nord (Defence Innovation Accelerator for the North Atlantic, DIANA) de l'OTAN. Elle peut également participer aux Capability Technology Groups (CapTechs) de l'Agence européenne de défense (AED) et au Hub for EU Defence Innovation (HEDI). La Suisse est toutefois exclue des projets du Fonds européen de défense (FED). Au DDPS, les espaces d'innovation du DDPS ainsi que le système d'innovation de la Défense sont soutenus par la recherche.

2.4 Principes de mise en œuvre stratégiques

Six principes de mise en œuvre stratégique constituent la base de la sélection des axes de recherche et de la mise en œuvre opérationnelle des activités de recherche dans le cadre du PRLT 2025-2028.

Orientation vers l'utilisateur

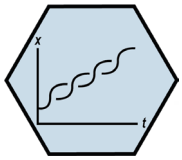
La recherche d'armasuisse est axée sur l'utilisateur, en particulier pour l'exécution de la mission des domaines départementaux Défense et armasuisse. Dans ce contexte, les priorités de la recherche s'orientent sur les capacités opérationnelles et leur mise en œuvre dans le cadre du développement des forces orienté capacités. En outre, la recherche doit être axée sur l'efficacité et l'efficience. Les résultats de la recherche doivent pouvoir être utilisés efficacement pour les différentes missions de l'armée et de ses organisations de soutien. La recherche se concentre sur les compétences technico-scientifiques nécessaires pour évaluer, d'un point de vue technologique, les options de développement dans les différents domaines de capacités. Ces compétences sont tout aussi pertinentes pour accompagner les mesures de mise en œuvre, notamment l'acquisition d'armement. Des compétences méthodologiques dans le domaine de la modélisation et de la simulation soutiennent ces activités et montrent l'utilité et les limites des nouvelles technologies dans l'environnement militaire. Ainsi, elles servent également de base de décision pour les réflexions doctrinales. Afin que les développements technologiques et les besoins de l'armée puissent être harmonisés au mieux, la recherche doit être capable de s'adapter. Elle peut ainsi s'ajuster en présence de changements éven-

tuels. Une évaluation annuelle des besoins permet de garantir que des adaptations du contenu de la recherche pourront être effectuées chaque année.

Degré de maturité de la technologie

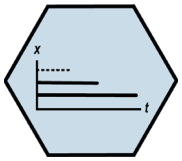
La recherche d'armasuisse assure la compétence technico-scientifique par le biais d'activités telles que la prospective technologique, les programmes thématiques et la mise à disposition de démonstrateurs. Dans ce contexte, la recherche d'armasuisse se concentre sur les degrés de maturité technologique 3 (preuve de l'aptitude au fonctionnement d'une technologie) à 5 (montage expérimental dans un environnement opérationnel) selon le modèle Technology Readiness Level (TRL) de la NASA. Le développement de prototypes (TRL 6) jusqu'au système qualifié avec preuve de l'utilisation réussie (TRL 9) n'est toutefois pas l'objet de la recherche d'armasuisse. Il doit être effectué ou mandaté par la planification de l'armée et les services d'achat dans le cadre du processus d'armement, par le biais du système d'innovation D ou des espaces d'innovation du DDPS.

Cycle de vie de la technologie



Le cycle de vie des technologies peut être comparé au cycle de vie des produits et a un impact direct sur les options stratégiques. Une technologie d'avenir peut devenir une technologie clé avant de devenir une technologie de base susceptible d'être supplantée par de nouvelles technologies innovantes. Dans le domaine civil, le cycle de vie des technologies s'est fortement accéléré ces dernières années. Dans le domaine militaire, le passage d'une technologie à l'autre est souvent plus coûteux. Comme les systèmes sont souvent en service depuis longtemps, l'intégration de nouvelles technologies par des sous-systèmes est un défi. La recherche d'armasuisse se concentre avant tout sur les phases de croissance et de maturité des technologies clés, car c'est pendant ces phases que l'on peut s'attendre à des progrès efficaces en vue d'une utilisation pour des armements. L'intégration dans des plateformes existantes est alors également prise en compte. La connaissance du cycle de vie des technologies réduit le risque d'introduire des technologies au mauvais moment et évite les mauvais investissements.

Horizon temporel à moyen et long terme

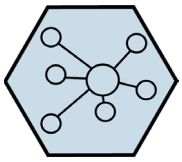


La recherche d'armasuisse sert à développer et à garantir les compétences technico-scientifiques nécessaires au maintien de la capacité d'expertise et de conseil dans le contexte de la politique de sécurité. Le besoin de ces capacités est déterminé par le développement des forces orienté capacités et les missions spécifiques de l'armée. Il peut inclure l'évaluation de menaces technologiques et de technologies alternatives. L'interaction entre les systèmes existants et futurs de l'armée est également cruciale pour garantir la compatibilité et la performance. Dans ce contexte, la recherche doit permettre d'identifier les tendances technologiques qui sont importantes pour la sécurité à long terme. Il s'agit en outre de suivre les progrès des technologies à potentiel disruptif dans les domaines civil et militaire. Ainsi, les technologies qui pourraient avoir un impact durable sur les capacités des forces armées sont identifiées et des mesures sont prises en temps voulu pour garantir la sécurité.

Des compétences grâce aux coopérations

La mise à disposition de compétences technico-scientifiques pour les instruments de la politique de sécurité requiert la collaboration d'acteurs toujours plus nombreux en raison de la complexité croissante de la mise en œuvre des tâches et des conditions-cadres économiques. Pour ce faire, des réseaux à long terme ont été et sont non seulement mis en place, mais aussi développés avec des partenaires issus de l'économie, de hautes écoles, d'autres institutions publiques et d'organisations internationales. L'objectif est d'optimiser l'utilisation des compétences existantes et d'assurer leur développement continu. Les partenariats stratégiques sont encouragés afin d'assurer la continuité du développement des compétences et de garantir la qualité des projets de coopération nationaux et internationaux. Les coopérations permettent d'accéder à des technologies clés, à des expériences en matière d'intervention et à des analyses techniques des menaces. Grâce aux compétences existantes des partenaires de coopération, il est possible de s'appuyer sur ces derniers pour réduire les coûts et permettre une utilisation efficace des ressources.

Mise en réseau multidisciplinaire



Les résultats de la recherche ont un impact direct sur les capacités opérationnelles de l'armée et sur les technologies des systèmes. Les systèmes de l'armée englobent aujourd'hui un grand nombre de technologies issues de différentes disciplines. C'est pourquoi il est important de toujours considérer le système dans son ensemble et de ne pas laisser les disciplines agir de manière cloisonnée. Pour y parvenir, des thèmes de recherche transversaux sont définis afin d'améliorer considérablement la qualité et les performances des systèmes ainsi que l'efficacité des exploitants, et de réduire ainsi le coût total.

2.5 Mandat légal et bases

Le mandat de recherche d'armasuisse découle principalement de la loi fédérale sur l'armée et l'administration militaire (art. 109, révision 2026), de l'ordonnance sur l'organisation du DDPS, de la politique d'armement du DDPS, des directives sur la collaboration entre les domaines départementaux Défense et armasuisse (CODA) et du plan intégré des tâches et des finances (PITF) armasuisse 2024-2026. Les bases légales pour la réalisation de la recherche de l'administration fédérale se trouvent dans la loi sur l'encouragement de la recherche et de l'innovation (LERI), ainsi que dans son ordonnance. Une liste détaillée des bases pertinentes à prendre en compte dans le cadre de la recherche d'armasuisse figure à l'annexe 2.

2.6 Rétrospective de la période 2021-2024

Sur la base du plan de recherche à long terme 2021-2024, les axes de recherche « Prospective technologique », « Technologies au service des capacités opérationnelles », « Intégration technologique pour systèmes d'intervention » et « Innovation & thèmes transversaux » ont fait l'objet d'un traitement systématiquement, et les enseignements tirés ont été mis à profit sous forme de prestations d'expertise et de prestations de conseil. Le but était de venir en appui aux organes concernés du DDPS, dans les questions technologiques, par des compétences techniques et scientifiques, depuis la planification jusqu'à l'élimination de l'équipement matériel de l'armée. Le transfert de connaissances de la recherche vers les processus de planification de l'armée a pu être amélioré grâce à une bonne collaboration avec l'état-major de l'armée et d'autres unités organisationnelles. Grâce à l'échange établi avec la planification de l'armée, la doctrine militaire et la troupe, il a également été possible d'orienter en permanence les programmes de recherche et les champs de compétences correspondants vers les besoins de la défense.

Au cours de la période 2021-2024, le Centre suisse des drones et de la robotique (CSDR) nouvellement établi a apporté son soutien à l'Armée suisse ainsi qu'à d'autres autorités en matière de robotique dans le domaine de la sécurité. Un accord de collaboration avec l'École polytechnique fédérale de Zurich (EPFZ) a été signé pour le programme commun de robotique de sécurité. La mise en place du Cyber-Defence Campus s'est poursuivie avec pour objectif d'identifier les cyberrisques émergents et de concevoir des solutions innovantes afin de contrer efficacement les menaces dans le cyberespace. En outre, en raison de son importance croissante pour l'armée, un nouveau programme de recherche a été lancé en 2022 pour le domaine spatial afin de suivre le développement fulgurant des technologies et d'acquérir des compétences dans ce domaine. Concernant le conseil stratégique, le DDPS a créé un conseil technologique avec l'EPF de Zurich (EPFZ). En outre, les espaces d'innovation du DDPS ont vu le jour au cours de la période 2021-2024 afin d'identifier, de développer et de tester de manière transdisciplinaire des solutions inédites pour répondre aux défis du département. Cette approche doit permettre de tirer à un stade précoce des enseignements pour des projets ultérieurs et d'éviter ainsi des erreurs d'investissement majeures.

2.7 Défis et actions requises

Le Conseil national et le Conseil des États ont décidé au printemps 2022 d'augmenter progressivement les dépenses de l'armée à partir de 2023, de sorte qu'elles représentent au moins 1% du produit intérieur brut d'ici 2030. En raison des déficits structurels des années 2024 à 2026, le Conseil fédéral envisage toutefois un aplatissement de l'évolution de la croissance et une prolongation jusqu'en 2035. Avec la planification actuelle des investissements pour les années 2023 à 2035, l'armée souhaite combler ses lacunes en matière d'équipement et augmenter sa capacité à durer.

Le budget de l'armée (en principe croissant) offre la possibilité d'anticiper les acquisitions d'armement, mais il comporte également de nombreux défis. Outre une charge de travail accrue pour la réalisation des projets d'acquisition, les exigences en matière de connaissances technologiques augmentent en parallèle. Le progrès technologique implique des cycles d'inno-

vation courts, ce qui représente un grand défi pour la planification et l'utilisation prévues sur le long terme des systèmes de l'armée. Les processus d'acquisition doivent être accélérés et simplifiés afin de pouvoir suivre le rythme de l'évolution technologique. Plusieurs recommandations ont été formulées par le cabinet de conseil Deloitte suite à son analyse du processus d'acquisition. Il a notamment été recommandé de mettre en place un processus simplifié pour les projets présentant des cycles d'innovation très courts. En outre, il a été signalé qu'il fallait exploiter la marge de manœuvre accrue offerte par la révision du droit des marchés publics. Pour pouvoir continuer à réagir à l'avenir aux développements technologiques et aux événements politiques mondiaux, toutes les parties prenantes devront faire preuve d'une certaine flexibilité.

La numérisation continuera à jouer un rôle important. C'est pourquoi la vision de l'armée suisse est aussi d'exploiter le potentiel de la numérisation et de l'intégrer dans la culture. La transformation numérique permet d'une part de rendre les processus plus efficaces et plus simples. D'autre part, la numérisation permet aussi d'avoir une longueur d'avance en termes de connaissances et de décisions. Pour mettre en œuvre la numérisation et maîtriser la complexité croissante qui y est associée, il est essentiel de comprendre les technologies et de pouvoir les évaluer. Il est en outre indispensable de protéger l'ensemble de l'infrastructure numérique contre les cyberattaques et les pannes.

Ces dernières années, les progrès techniques ont été énormes et ils continueront à s'accroître. Divers instruments permettent de rester à la pointe de la technologie et de la science et d'exploiter pour l'armée les enseignements obtenus. La prospective technologique permet d'identifier en temps voulu les tendances technologiques et les technologies disruptives et d'évaluer leur impact sur les forces armées. Des thèmes sélectionnés pertinents d'un point de vue militaire peuvent ensuite être étudiés plus en détail dans le cadre de projets de recherche. Le développement des compétences par la recherche est une condition préalable à la fourniture d'expertises pour l'armée et les achats. Du fait de la rapidité des changements technologiques, les exigences envers la gestion des technologies de l'armée sont également élevées. C'est pourquoi il y a lieu de garantir le transfert, au profit de l'armée, des connaissances et des enseignements tirés de la recherche. Des feuilles de route technologiques peuvent ainsi être établies pour soutenir la planification stratégique. Le potentiel et le caractère disruptif des nouvelles technologies peuvent être mis en évidence à l'aide de démonstrateurs dans des scénarios proches de la réalité, qui correspondent dans une large mesure à l'environnement des engagements de l'armée. Des simulations et des réalités virtuelles peuvent également être utilisées pour la démonstration de technologies modernes. En dehors des aspects technologiques, des questions de fond sociales et éthiques se posent souvent quant à l'utilisation de technologies modernes, notamment l'intelligence artificielle et les systèmes autonomes. Ici, les discussions interdisciplinaires doivent être encouragées et soutenues, mais doivent également être intégrées dans la mise en œuvre des thèmes de recherche. Il convient en outre de veiller à ce que les enseignements tirés de ces discussions soient intégrés dans la formation et l'entraînement des soldats et des cadres.

L'introduction de l'instrument que sont les espaces d'innovation a constitué une autre recommandation du rapport Deloitte. Contrairement à la recherche, l'innovation a pour objectif de trouver de nouvelles solutions répondant à un besoin concret et de les tester dans un environnement proche des conditions d'utilisation, et ce dans un délai raisonnable. La recherche apporte toutefois une contribution importante aux processus d'innovation. Souvent, l'innovation consiste à adapter et à utiliser des solutions civiles existantes pour l'environnement militaire.

3 Axes de recherche et domaines thématiques prioritaires 2025-2028

La recherche d'armasuisse a pour but de développer les compétences technico-scientifiques nécessaires pour soutenir le développement des forces orienté capacités du Groupement Défense et les processus d'acquisition d'armasuisse. En outre, il s'agit de créer les bases de compétences permettant d'évaluer et de mettre en œuvre des projets d'innovation en faveur du DDPS. Quatre axes de recherche et respectivement deux ou trois domaines thématiques prioritaires correspondants ont été définis pour l'orientation future de la recherche (Illustration 7).

- L'axe de recherche **« Prospective technologique »** sert à détecter à un stade précoce les développements technologiques qui ont une influence potentielle sur la sécurité de la Suisse. L'accent n'est pas seulement mis sur la surveillance des développements technologiques, mais aussi sur l'évaluation de l'impact technologique, qui met en évidence les conséquences sur la société, l'économie et les instruments de la politique de sécurité. Il s'agit d'identifier à un stade précoce le potentiel disruptif des développements technologiques et d'anticiper les opportunités et les menaces qui y sont liées dans le contexte de la politique de sécurité.

- L'axe de recherche **« Technologies pour les capacités opérationnelles »** se compose de trois domaines thématiques prioritaires, qui visent en premier lieu à développer des compétences pour soutenir le développement des forces orienté capacités. Sont ici prioritaires les domaines thématiques « Impact et protection dans l'espace physique », « Opérations et protection dans le cyberespace et l'espace électromagnétique » ainsi que « Technologies pour garantir la supériorité de l'information ». Cette orientation doit permettre de maintenir à jour les connaissances technologi-

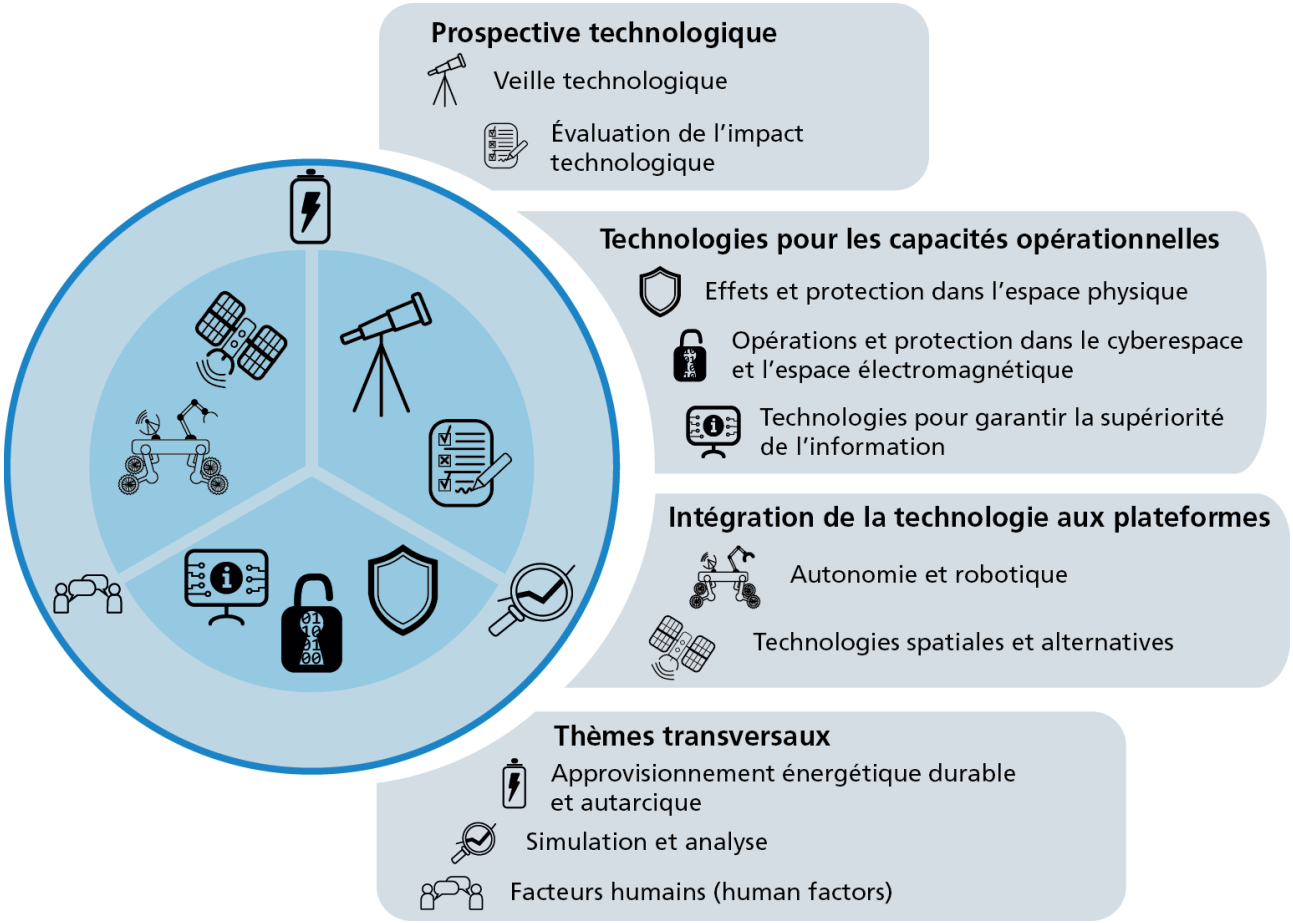


Illustration 7: Axes de recherche et domaines thématiques prioritaires du PRLT 2025-2028.

ques nécessaires à la conception d'un réseau moderne et intégré de capteurs, de renseignement, de conduite et d'action (CRCA) et de poursuivre ainsi, entre autres, la vision d'une armée suisse numérisée.

- L'axe de recherche **« Intégration de la technologie aux plateformes »** a pour objectif d'intégrer différentes technologies dans une plateforme afin de fournir des démonstrateurs qui peuvent mettre en évidence le potentiel des technologies en laboratoire ou dans un environnement proche des conditions d'utilisation. Ces plateformes ont le potentiel pour couvrir plusieurs capacités opérationnelles en même temps. Le domaine « Autonomie et robotique » est un domaine thématique prioritaire important de cet axe de recherche. Il met en évidence les possibilités d'utilisation de systèmes robotiques sur terre, dans l'eau et dans les airs. Le deuxième domaine thématique prioritaire se concentre sur les « Technologies spatiales et alternatives ». Il vise à déterminer comment la sphère d'opération représentée par l'espace exoatmosphérique peut être utilisée de manière ciblée pour un petit État comme la Suisse d'un point de vue militaire et comment des alternatives peuvent compenser les pannes ou les limitations des services basés sur les satellites. L'axe de recherche « Intégration de la technologie aux plateformes » joue un rôle important de passerelle pour soutenir les espaces d'innovation du DDPS et le système d'innovation de la Défense.
- L'axe de recherche **« Thèmes transversaux »** se concentre sur le développement de compétences dans des domaines thématiques indispensables à la fourniture de prestations par les forces de sécurité. Ainsi, des connaissances concernant l'« Approvisionnement énergétique durable et autarcique » sont très importantes si le DDPS veut apporter une contribution notable aux objectifs climatiques de la Confédération tout en remplissant ses missions dans des situations extraordinaires. Le domaine thématique prioritaire « Simulation et analyse » permet de fournir les bases pour le développement des forces armées et de développer le concept d'un environnement de simulation holistique de l'Armée suisse. L'armée est un système socio-technique dans lequel l'homme et la complexité qui en découle jouent un rôle essentiel. C'est pourquoi le domaine thématique prioritaire « Facteurs humains » concerne aussi bien l'interaction entre l'homme et la technique que les aspects sociaux qui doivent être pris en compte lors de l'utilisation des technologies dans le contexte des forces armées.

Le PRLT 2025-2028 est axé sur les besoins des différents instruments de la politique de sécurité. L'Illustration 7 présente une vue d'ensemble des axes de recherche et des domaines thématiques prioritaires. Ils sont présentés en détail ci-dessous et expliqués du point de vue de l'utilité et de l'orientation vers l'utilisateur.

3.1 Prospective technologique

3.1.1 Veille technologique

Situation de départ et problématique

L'évolution technologique actuelle est très rapide et la numérisation, en particulier, a entraîné un afflux de nouveaux produits et applications. On observe que deux écosystèmes semblent se former en fonction des sphères d'influence de la politique d'hégémonie mondiale, au centre desquels se trouvent les États-Unis et la Chine. C'est pourquoi les développements technologiques ne sont pas seulement dynamiques et parfois complémentaires, mais aussi parallèles dans certains domaines. Sur les marchés, le remplacement d'une technologie par une autre est souvent perçu comme un gain de performance. Le nombre de ces cycles technologiques a massivement augmenté au cours des dernières décennies et ils se produisent à des intervalles de plus en plus courts. De plus, les différentes technologies ne se développent pas isolément les unes des autres. Très souvent, la disponibilité d'une technologie particulière entraîne le progrès d'une autre technologie, ce qui peut conduire à une réaction en chaîne d'avancées dans d'autres secteurs technologiques. Ce phénomène impose des exigences très strictes concernant la prospective technologique.

Aujourd'hui, le rythme des progrès technologiques est déterminé, dans de nombreux domaines, par la demande attendue des marchés civils. Même si de nombreuses technologies modernes présentent bien un potentiel d'application militaire, leur utilisation dans les forces armées est nettement moins avancée. Cela s'explique particulièrement par la longue durée d'utilisation des systèmes principaux (généralement entre 20 et 40 ans). Nous nous efforçons de rester au niveau technologique actuel grâce au maintien de la valeur, mais les possibilités civiles d'utilisation de la technologie progressent de plus en plus rapidement. De plus, l'environnement opérationnel des forces armées impose des exigences très élevées en matière de robustesse, de disponibilité et de sécurité. Le marché des biens militaires est plus petit que le marché civil et souvent contrôlé par l'État, de sorte que l'industrie de l'armement n'entre en jeu que lorsque la demande des forces armées est suffisamment importante et que celles-ci sont également prêtes à financer les développements correspondants. Ces raisons font que les technologies utilisées dans les moyens d'intervention des forces armées ne correspondent généralement pas au niveau disponible dans les produits civils de la vie quotidienne.

La complexité et les exigences particulières de l'environnement militaire requièrent une surveillance systématique des développements technologiques. Il convient de distinguer deux horizons temporels différents pour la prospective technologique. Alors qu'un large horizon temporel est fixé lors de la veille technologique, l'évaluation de l'impact technologique est plutôt axée sur le long terme. La veille technologique, avec ses deux éléments principaux que sont le suivi de la technologie et du marché, constitue la base d'évaluation des technologies en ce qui concerne leur degré de maturité et leur potentiel d'utilisation. Sur cette base, les forces armées peuvent être conseillées sur l'opportunité de miser sur une nouvelle technologie et sur le moment idéal pour le faire. Cela permet de s'assurer que les ressources financières sont investies efficacement dans les technologies modernes. En revanche, les enseignements tirés de l'évaluation de l'impact technologique sont destinés à soutenir les processus de développement à long terme des forces armées. Dans les deux cas, il convient de suivre en permanence les tendances et les développements actuels.

L'objectif d'une surveillance globale des développements technologiques est de consolider les informations issues des activités de recherche en cours et d'identifier les technologies qui se retrouvent, d'un point de vue thématique, en dehors de l'orientation des programmes de recherche en cours, mais qui peuvent néanmoins devenir pertinentes pour l'accomplissement des missions des forces de sécurité. C'est pourquoi la veille technologique doit être comprise de manière très large. Elle regroupe des technologies principalement civiles mais aussi militaires dans une vue d'ensemble technologique sur 360° qui fait l'objet d'une évaluation. Comme les technologies peuvent par définition être considérées de manière assez universelle, il existe à ce sujet quelques bonnes études récentes et complètes au niveau international. Une tâche essentielle est d'interpréter et de présenter les enseignements tirés de ces études dans le contexte de la politique de sécurité suisse et de ses instruments.

Thèmes de recherche 2025-2028

Surveillance des développements technologiques

- Identification de moteurs technologiques pertinents pour la sécurité de la Suisse
- Suivi de développements technologiques civils présentant un potentiel pour une utilisation militaire
- Développement d'une plateforme d'analyse pour la détection automatique des développements technologiques rapides et disruptifs
- Élaboration d'une représentation intuitive de moteurs technologiques
- Mise en place d'un réseau international de suivi et d'évaluation de développements technologiques

Évaluation des développements technologiques

- Estimation de la maturité des technologies essentielles en matière de sécurité et évaluation de leur applicabilité future pour les forces d'intervention
- Évaluation du potentiel disruptif des technologies
- Détermination du cycle de vie technologique de produits importants pour d'un point de vue militaire
- Mise en place de méthodes pour la détection précoce et la gestion d'événements inattendus ayant des conséquences importantes (événements Black Swan)
- Élaboration de contributions pour l'orientation de la recherche dans le domaine important pour la sécurité

3.1.2 Évaluation de l'impact technologique

Situation de départ et problématique

L'évaluation de l'impact technologique s'intéresse aux conséquences des développements technologiques sur les aspects sociologiques les plus divers, qui fournissent à leur tour le cadre d'une future politique de sécurité et de la conception de ses instruments. En ce sens, l'évaluation de l'impact technologique sert à anticiper les scénarios d'avenir possibles, ceux-ci se focalisant finalement sur des thèmes liés à la sécurité nationale en général et sur l'organisation des forces armées en particulier.

Dans le cadre de l'évaluation de l'impact technologique, l'une des priorités est d'identifier les technologies présentant un fort potentiel disruptif et d'anticiper les conséquences possibles, que ce soit dans le contexte militaire ou dans le contexte civil. Les deux sont nécessaires, car les deux domaines s'influencent mutuellement. Dans l'environnement civil par exemple, nous avons déjà expérimenté de telles disruptions dans le cadre de la progression de la numérisation. Les plateformes numériques, qui se sont positionnées comme des intermédiaires entre les clients et les prestataires, ont bouleversé les modèles d'affaires de secteurs entiers. Les entreprises établies qui sont passées à côté de la numérisation ont disparu. La numérisation rend également visibles des changements sociaux qui se traduisent par exemple par de nouvelles formes numériques d'interaction entre les individus ou les groupes. La numérisation n'a pas encore autant progressé au sein des forces armées que dans l'environnement civil. Il faut toutefois s'attendre à ce que la progression de la numérisation au sein des forces armées entraîne des disruptions d'une ampleur similaire à celles que nous connaissons dans la vie quotidienne civile. Il est essentiel d'identifier en temps voulu les évolutions disruptives afin d'en tirer les conséquences qui s'imposent pour le développement des forces orienté capacités et de réduire les risques.

L'évaluation de l'impact technologique dans le contexte de la politique de sécurité doit adopter une approche holistique afin de déterminer les actions requises

possibles dans différents scénarios d'avenir. Il ne s'agit pas d'évaluer les scénarios d'avenir en fonction de leur probabilité de survenance, mais d'y réfléchir afin de poser les bases de futures options d'action. La gestion d'éventuelles disruptions qui peuvent survenir en raison des évolutions technologiques constitue le défi le plus important à cet égard. Pour cela, une réflexion transdisciplinaire ouverte tenant compte de l'interaction entre la technologie, l'économie, la société, le droit, l'éthique, l'écologie et la politique est nécessaire.

L'évaluation de l'impact technologique peut ainsi contribuer à l'anticipation de scénarios futurs possibles et donc de crises éventuelles, comme l'exige le rapport sur la politique de sécurité. Cependant, les résultats pourraient également être partagés au niveau interdépartemental et avec d'autres acteurs intéressés par un échange sur les développements futurs possibles dans leurs domaines d'intérêt. Pour évaluer l'impact de nouvelles technologies, il convient de considérer aussi bien les opportunités potentielles que les menaces. Des opportunités se présentent lorsque les missions de l'armée sont accomplies de manière plus efficace ou lorsque l'utilisation de nouvelles technologies apporte un avantage opérationnel et donc une supériorité opérationnelle. L'éventail des menaces potentielles peut être très large. Dans le cadre de l'évaluation de l'impact technologique, il s'agit d'identifier les menaces qui, par leurs conséquences, peuvent causer des dommages importants à la société, restreindre la capacité d'action souveraine de l'État ou limiter l'armée dans l'accomplissement de sa mission.

Dans ce contexte, l'évaluation de l'impact technologique doit permettre d'établir une base d'anticipation pour le développement des forces orienté capacités, dans le but de réduire les risques de planification à long terme. Il s'agit de clarifier le potentiel des technologies émergentes et disruptives dans des scénarios d'avenir à l'aide de simulations et de jeux de guerre, et de montrer les conséquences de leur utilisation.

Thèmes de recherche 2025-2028

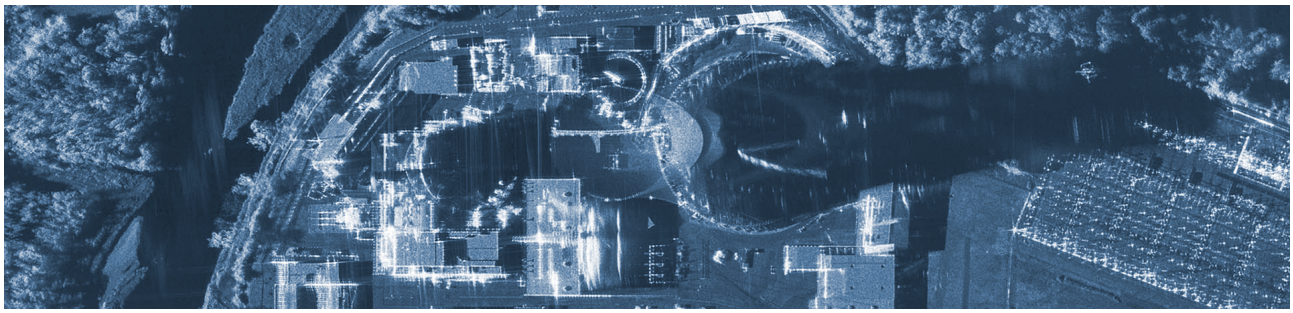
Développement de scénarios

- Mise en place de méthodes et de techniques de créativité pour le développement de scénarios et l'analyse d'évaluations de l'impact technologique, et transformation en recommandations d'actions stratégiques
- Développement de narratifs pour illustrer la disruption technologique dans des scénarios importants du point de vue de la sécurité
- Utilisation d'approches visionnaires et spéculatives pour identifier et diffuser de futurs développements technologiques et leur potentiel d'application
- Développement de futurs profils de compétences pour les différentes fonctions au sein de l'armée
- Création d'un réseau d'experts avec une participation internationale
- Analyse des conséquences des développements technologiques par rapport aux aspects politiques, économiques, socioculturels, écologiques, géographiques et juridiques (PESTEL)

Simulation et jeu de guerre

- Développement de méthodes de jeu de guerre axées sur les technologies d'avenir présentant un potentiel de disruption
- Mise en œuvre de scénarios par des simulations numériques avec prise en compte des technologies d'avenir
- Mise en place d'un réseau suisse d'experts pour anticiper les développements technologiques

3.2 Technologies pour les capacités opérationnelles



3.2.1 Effets et protection dans l'espace physique

Situation de départ et problématique

L'armée ne peut remplir sa mission que si elle est en mesure d'agir de manière coordonnée et synchronisée dans toutes les sphères d'opération, de la manière la plus adaptée à la situation actuelle. On parle alors d'opérations multidomaines. Celles-ci impliquent, d'une part, la capacité d'atteindre des objectifs opérationnels par des actions tactiques. D'autre part, cela doit être rendu impossible pour la partie adverse. Aujourd'hui déjà et très probablement à l'avenir, les actions de combat ont principalement lieu dans les zones construites et seulement partiellement évacuées. Il en découle naturellement des exigences très élevées en matière de précision et d'évolutivité des propres moyens d'action. D'une part, il s'agit d'obtenir un effet maximal sur ce terrain exigeant et, d'autre part, de ne causer que des dommages collatéraux minimaux, en particulier lorsque des infrastructures et un espace vital propres sont également concernés. Pour qu'un objectif puisse être atteint de la manière prévue, il est indispensable que le CRCA soit rapide. C'est le résultat d'une interaction réussie entre une image actuelle de la situation, une acquisition rapide du but, une direction précise du feu ainsi qu'une précision technique du ciblage et une résistance aux perturbations électromagnétiques du moyen d'action. Afin de maximiser la liberté d'action et la capacité à durer, il convient en outre d'accorder une importance centrale à la protection du personnel, du matériel et de l'infrastructure de l'armée, et notamment parce que les sites possibles de l'armée devraient être largement explorés bien avant le déclenchement d'actions de combat concrètes.

Effets dans l'espace physique

Pour obtenir un effet maximal avec des moyens limités, il faut une composition optimisée des formations. En considérant les facteurs de réussite classiques tels que la mobilité, l'efficacité et la vulnérabilité des systèmes, la précision au moyen d'une navigation autonome et la portée des moyens d'action, il est possible de tirer des conclusions sur la valeur opérationnelle des formations. En adaptant les tendances actuelles du développement des forces armées et de la recherche dans le domaine des systèmes d'armes aux conditions suisses et en les calculant pour différents scénarios d'engagement, il est possible de concentrer les clarifications supplémentaires et les propres activités de recherche sur les variantes les plus prometteuses.

Les progrès réalisés dans les technologies du CRCA permettent d'augmenter considérablement l'efficacité et l'efficience des engagements. Parallèlement, le niveau des exigences envers la mobilité et l'autonomie des systèmes est toujours plus élevé. Dans le domaine du tir courbe, cela signifie par exemple que les pièces d'artillerie opèrent de plus en plus de manière autonome et qu'elles sont regroupées en unités de feu sur de plus grandes distances en fonction de l'engagement. Cela permet certes de réduire la vulnérabilité de chaque pièce d'artillerie, mais en même temps, les exigences en matière de mise en réseau et de direction du feu augmentent considérablement. L'utilisation décentralisée d'effecteurs peut encore être optimisée grâce à l'utilisation de différents systèmes à portée échelonnée et de munitions de précision. La munition rôdeuse (loitering munition) pousse le principe d'engagement des effecteurs décentralisés à son paroxysme, en ce sens que l'effecteur reste au-dessus de la zone cible pendant une période prolongée, soit en combattant de manière autonome un objectif identifié, soit en attendant l'acquisition d'un but. Les munitions intelligentes, par exemple les drones d'attaque ou, justement, les munitions rôdeuses, pourraient également

servir pour une utilisation autonome ou semi-autonome ciblée contre des objectifs très spécifiques, comme les systèmes radars ou les systèmes de communication. La lutte contre ces moyens d'action autonomes intelligents et ces munitions de précision constitue un autre grand axe parmi les développements actuels. Même si on utilise traditionnellement des moyens de défense sol-air, ces systèmes manquent pourtant de précision ou sont trop inertes - selon les menaces. Les développements technologiques – sous l'impulsion des civils – des sources laser et de l'optique adaptée font entrer les lasers comme armes dans le champ des applications possibles. Les avantages des armes à laser sont nombreux : elles sont par ex. très précises, rapidement utilisables, réutilisables à l'infini, modulables concernant leur effet, présentent une faible signature et peuvent être exploitées sans munitions. En revanche, la mise à disposition d'une quantité suffisante d'énergie et la gestion des conditions météorologiques constituent un défi de taille. La technologie laser est également adaptée à l'éblouissement des capteurs. Il faut notamment penser à la lutte contre les munitions intelligentes et les moyens d'exploration spatiaux.

Les micro-ondes conviennent également pour produire un effet ciblé. En outre, elles agissent elles-aussi de manière invisible et silencieuse. Grâce aux micro-ondes, il est possible de perturber temporairement ou d'endommager durablement sur de courtes distances des composants électroniques ainsi que des drones. Dans le contexte militaire, des armes à micro-ondes, appelées systèmes HPM (High Power Microwave), sont disponibles sur le marché. Elles appartiennent à la catégorie des Directed Energy Weapons (armes à énergie dirigée), qui peuvent mettre des cibles hors service, les endommager ou les détruire en concentrant l'énergie.

Protection dans l'espace physique

Pour les forces armées modernes, la compétence fondamentale de l'autoprotection est indispensable pour garantir la capacité de survie, de façon à assurer l'accomplissement des missions. Les conditions d'engagement, les développements technologiques généraux, par exemple les nouveaux matériaux, et les caractéristiques des moyens d'action létaux ou non létaux de l'adversaire déterminent l'étendue et la portée de la protection requise. Alors que les plastiques et les céramiques modernes permettent de réduire sensiblement le poids des systèmes de protection corporelle tout en conservant la même efficacité de protection, le potentiel des plateformes mobiles semble en grande partie épuisé. En conséquence, on constate dans ce domaine un déplacement des activités de développement et de recherche vers des solutions de protection réactives et, de plus en plus souvent, également actives. Les solutions de protection spécialement actives promettent une nette amélioration de l'efficacité de protection tout en conservant au maximum un poids stable. Les deux variantes présentent toutefois l'inconvénient qu'elles peuvent – selon le principe de fonctionnement et la menace de référence – causer des dommages collatéraux considérables, et qu'il est nécessaire d'adapter les procédés d'engagement utilisés jusqu'ici.

La menace que représentent les missiles balistiques n'est pas nouvelle. La Suisse ne peut se défendre contre ces missiles que dans le cadre d'une coopération internationale. Les systèmes de vol et de missiles hypersoniques représentent une nouvelle catégorie d'armes à longue portée ; en raison de leur trajectoire de vol proche de la terre, ils ne peuvent être détectés par les moyens de reconnaissance terrestres et aéroportés que quelques minutes avant d'atteindre leur cible. La vitesse élevée et la vaste zone de buts qui en découle, combinées aux contraintes de temps, constituent des défis majeurs pour la défense contre les armes hypersoniques, même pour les nations de haute technologie disposant de vastes compétences en matière d'armement. De plus, les pays occidentaux ont réactivé ou intensifié leurs propres programmes de développement d'armes hypersoniques. Même si l'on s'attend à ce que l'utilisation de telles armes se limitera – du fait de leur coût élevé – à des cibles d'une grande importance stratégique ou symbolique, il convient d'observer leur évolution par rapport aux concepts de protection possibles. Les installations fixes telles que les infrastructures militaires en Suisse et à l'étranger, les infrastructures critiques et les installations des services de base sont vulnérables aussi bien dans les conflits armés que dans les conflits hybrides.

Le risque toujours élevé d'attentats terroristes a renforcé la sensibilité aux dangers de l'utilisation d'armes biologiques, chimiques et radiologiques. En raison de leur potentiel de nuisance, la protection contre les agents biologiques de combat et les biotoxines, qui sont en principe interdits à l'échelle internationale, doit être évaluée. Comme ces agents de combat réagissent très rapidement aux influences de l'environnement, la recherche sert à identifier et à détecter les substances biologiques et chimiques à l'aide de capteurs et à développer des mesures de protection et de défense appropriées. Les progrès de la biotechnologie et du génie génétique, ainsi que leur accessibilité,

sont particulièrement importants à cet égard. La possibilité de modifier les propriétés d'organismes offre des opportunités pour une meilleure protection, mais représente également un risque de nouveaux agents de combat. Dans le cas des armes radiologiques, les substances radioactives sont libérées par des explosifs conventionnels. Les mesures de protection sont les mêmes que celles qui doivent être prises en cas de rejets de substances radioactives dus à des accidents de centrales nucléaires.

Malgré les progrès réalisés dans la détection et la neutralisation de charges improvisées, appelées Improvised Explosive Devices (IED), les charges explosives improvisées représentent une menace latente pour les forces d'intervention et la population dans les situations de conflit. Il est donc important de continuer à améliorer la détection des IED et les éventuelles techniques de neutralisation. Comme le montrent les expériences des zones d'engagement, la prévention des attentats peut être très efficace si l'on tente de détecter les anomalies dans la chaîne commerciale et logistique de composants et de substances spécifiques utilisés pour la réalisation d'IED. Cela permet d'identifier les fabricants d'IED et de les neutraliser avant qu'une action violente ne soit déclenchée.

L'utilisation de drones (semi-)autonomes comme moyen de transport pour les IED, enrichis ou non de substances biologiques, chimiques ou radiologiques, constitue une menace récente et un défi considérable. En raison de leur petite taille, il est non seulement difficile de les détecter à temps, mais une lutte à une distance de sécurité par rapport à leur objectif d'attaque est actuellement une question non résolue.

Les actions dans le cyberespace et l'espace électromagnétique contribuent également de manière significative à la protection dans l'espace physique. La protection contre les interférences électromagnétiques (IEM), les armes à micro-ondes (HPM) et les cyberattaques est importante pour protéger les infrastructures critiques. Celles-ci présentent souvent une forte interdépendance, ce qui peut entraîner des réactions en chaîne en cas d'attaque contre un ou plusieurs éléments d'infrastructure. Ces interdépendances et leurs risques doivent être étudiés et décrits avec précision afin que des mesures efficaces puissent être prises pour limiter et gérer les événements dommageables. Les champs électromagnétiques peuvent également être utilisés contre les personnes afin d'influencer négativement leurs performances. C'est pourquoi non seulement les infrastructures et les équipements, mais aussi les personnes doivent être protégés contre les puissants rayonnements électromagnétiques.

La protection la plus efficace est toutefois obtenue en dissimulant ses propres moyens aux yeux de la reconnaissance adverse. Le camouflage et le leurrage multispectraux constituent des approches efficaces à cet égard. Aujourd'hui, on peut partir du principe que la plupart des installations fixes ont fait l'objet d'une reconnaissance et que leurs coordonnées sont connues. En revanche, les objets mobiles peuvent être camouflés en adaptant leur signature électromagnétique à l'environnement et en supprimant les émissions telles que le bruit ou la fumée. Il est ainsi plus difficile pour un adversaire de les localiser, de les identifier et de les suivre. La technologie de l'enveloppe de camouflage est utilisée pour réduire la signature radar, en particulier dans l'aéronautique, mais aussi de plus en plus sur les plates-formes maritimes et terrestres. Cet effet de furtivité est obtenu par l'utilisation de certains matériaux composites, par l'utilisation de matériaux et de revêtements absorbant les ondes radar ou par des constructions de plateformes spécifiques. Le morphing sert le même objectif pour modifier les propriétés de la surface, comme l'adaptation de la couleur, ou la modification des structures de la surface, comme la modification d'une aile d'avion en vol.

Thèmes de recherche 2025-2028

Protection des véhicules, des avions et des personnes

- Étude de nouveaux matériaux pour améliorer la protection balistique des personnes
- Suivi des développements concernant la protection active et réactive de véhicules et développement de la capacité d'évaluation correspondante
- Étude de nouvelles approches dans le domaine du camouflage et du leurrage, et développement de la capacité d'évaluation pour les systèmes futurs
- Évolution des modèles de vulnérabilité de plateformes afin d'améliorer l'autoprotection et les procédés d'engagement
- Étude des technologies possibles pour une protection proactive contre les plateformes sans occupants (UAV/UGV)
- Étude et modélisation des effets et des dommages potentiels pouvant être causés par des charges improvisées afin de promouvoir la prise de conscience des risques, d'améliorer les procédés d'engagement et de soutenir la conception de la protection des plateformes et des infrastructures

Protection et sécurité des bâtiments et des infrastructures

- Étude et modélisation des mécanismes d'action des impulsions électromagnétiques et développement de directives pour la conception de solutions de protection correspondantes
- Étude et modélisation des dommages potentiels pouvant être causés par des grosses charges explosives afin de soutenir la planification de nouvelles infrastructures et d'améliorer les plans d'urgence des infrastructures existantes
- Soutien lors du développement de solutions pour la consolidation ultérieure des bâtiments contre les charges et les projectiles et pour l'augmentation du degré de protection des constructions existantes
- Suivi du développement dans le domaine de la défense contre les plateformes sans occupants (UAV/UGV) et développement de la capacité d'évaluation
- Analyse de l'évolution dans le domaine de la détection et de la défense contre les moyens d'action sol-sol afin de développer les connaissances pour les expertises

Effet

- Suivi des développements dans le domaine des armes hypersoniques en mettant plus particulièrement l'accent sur la manœuvrabilité et l'effet sur la cible, et analyse des contre-mesures possibles
- Suivi des développements concernant les systèmes d'armes autonomes en mettant l'accent sur les principes d'engagement, le pilotage et la coordination ainsi que la capacité d'action
- Simulation de systèmes sol-air et air-air, y compris modélisation des ogives pour optimiser leur utilisation
- Étude des bases d'un rayonnement électromagnétique dirigé avec une densité énergétique élevée afin de déterminer son potentiel d'action
- Élargissement des compétences balistiques aux systèmes modernes, en accordant une attention particulière au guidage en phase finale et à la propulsion des missiles
- Étude des possibilités d'amélioration de la direction du feu et de l'acquisition du but pour le tir courbe et les missiles d'artillerie, dans le but d'obtenir une transmission plus rapide et plus précise des informations entre le capteur et le moyen d'action
- Développement des compétences balistiques pour les opérations air-sol afin de soutenir le développement des capacités correspondantes

Sécurité des explosifs et des munitions

- Étude des caractéristiques d'initiation et de mise en œuvre des explosifs en vue de promouvoir la sécurité lors de la manipulation d'explosifs
- Étude du vieillissement des explosifs et des poudres de charge propulsive modernes afin d'optimiser les conditions de stockage et le calcul de la durée de vie des munitions et des explosifs
- Étude du processus de vieillissement des matériaux utilisés pour la protection balistique et détonique afin de prédire l'effet de protection tout au long de leur durée de vie
- Détermination de l'impact environnemental des munitions et des résidus de munitions dans le but d'optimiser l'assainissement des sites contaminés et de minimiser les dommages causés à la nature par l'utilisation de munitions et d'explosifs

3.2.2 Opérations et protection dans le cyberespace et l'espace électromagnétique

Situation de départ et problématique

Le cyberespace et l'espace électromagnétique (CYBEEM) occupent une grande place dans les conflits actuels. L'armée suisse et la société sont déjà régulièrement confrontées à des cyberattaques au quotidien, et la numérisation croissante accroît la vulnérabilité à ce type d'attaques. La nécessité de tenir compte de ces défis, tant dans l'évolution de l'armée qu'au niveau de la progression de la numérisation en Suisse, est indéniable. La conception générale Cyber du DDPS et la stratégie nationale de protection contre les cyberrisques (SNPC) présentent, dans ses grandes lignes, la manière de procéder. La conception générale Cyber se concentre à cet égard sur l'évolution de l'armée dans le domaine Cyber jusque dans les années 2030.

L'accent est mis sur l'obtention et le maintien d'une avance en matière d'information, dans l'optique d'un processus décisionnel supérieur dans le CYBEEM. Pour y parvenir, il convient de miser sur une forte auto-

protection (afin d'empêcher l'adversaire de prendre de l'avance), ainsi que sur des actions ou opérations ciblées. L'objectif est de confronter l'adversaire à des retards d'information et donc dans ses prises de décision. À long terme, ces deux domaines doivent être développés de manière significative par rapport à la situation actuelle : dans un premier temps, de manière centralisée et en tenant compte des infrastructures de base, et par la suite également de manière locale et autonome auprès d'unités sur le terrain.

Ce développement qualitatif et quantitatif fait face à de multiples défis, dont la plupart sont dus à la mise en réseau et à la numérisation croissantes, à l'évolution constante du cyberespace, à la courte durée de vie des technologies de l'information et de la communication (TIC) et au grand nombre de nouvelles technologies et d'innovations. Ainsi par exemple, un char de combat reste un système d'armes hautement protégé pour combattre directement des objectifs au sol. Mais il est également relié au CYBEEM par ses systèmes TIC et constitue donc un objectif d'attaque dans cet espace. Si ses systèmes TIC ont été atteints avec succès, le char devient même le point de départ d'attaques.

Pour faire face à ces défis et renforcer les capacités étatiques adéquates et l'autonomie dans le cyberespace, il est nécessaire d'unir les forces au moyen de coopérations nationales et de partenariats dans l'éducation, la recherche et l'économie. C'est la seule façon d'anticiper les développements technologiques pertinents et de former et d'attirer des professionnels pour répondre aux défis actuels et futurs. La recherche a un rôle central à jouer dans l'intégration des développements technologiques tant incrémentiels que disruptifs. En se penchant suffisamment tôt sur de tels développements, il est possible d'évaluer leurs opportunités et leurs risques concernant l'avance en matière d'information et les processus décisionnels supérieurs, et de les transformer rapidement en capacités opérationnelles dans le cadre d'acquisitions et de transferts de connaissances.

Autoprotection CYBEEM

L'armée, l'administration publique, l'infrastructure critique, l'économie et la société présentent un haut degré de connexion numérique, et de nombreux processus et capacités sont numérisés. L'Internet des objets (IdO) est devenu une réalité avec des véhicules et des appareils volants semi-autonomes, des capteurs en réseau pour contrôler des bâtiments, des réseaux électriques ou même des villes intelligentes entières. Cela comporte des opportunités et des risques. L'utilisation croissante de moyens d'information et de communication requiert des mesures de protection, notamment en ce qui concerne la disponibilité, l'intégrité et la confidentialité des systèmes d'information et de communication. Dans ce contexte, l'utilisation de logiciels civils et la chaîne de production de composants matériels importants avec des fonctions logicielles intégrées représentent un potentiel de vulnérabilité de l'infrastructure d'information et de communication qui est difficile à évaluer.

La mise en réseau et la numérisation continueront de progresser dans les années à venir, augmentant ainsi encore la fragilité du cyberespace. Les processus, les capacités et les technologies pour lesquels, pour diverses raisons, l'autoprotection dans le cyberespace n'a pas ou n'a guère joué de rôle jusqu'à présent, seront alors particulièrement vulnérables. Cela est par ex. dû au fait que ces processus, capacités et technologies n'étaient pas du tout numériques ou connectés auparavant (comme dans le cas des machines à café, des systèmes d'alarme ou des véhicules) ou que les cyberattaquants s'étaient alors heurtés à des obstacles techniques et financiers importants. Des processus, des capacités et des technologies entièrement nouveaux peuvent également présenter une vulnérabilité similaire. C'est par exemple le cas de nouveaux procédés et protocoles cryptographiques capables de résister aux attaques d'ordinateurs quantiques puissants. Si la conception d'ordinateurs quantiques suffisamment puissants devenait possible, il ne serait donc pas nécessaire de remplacer ou d'adapter tous les systèmes utilisant la cryptographie. Les ordinateurs quantiques rendront inutilisables les procédures asymétriques qui ne nécessitent pas l'échange préalable d'une clé. Mais comme elles font intégralement partie du quotidien (elles constituent par exemple la base de la sécurisation de la communication avec les services sur Internet), l'ordinateur quantique a ici clairement un potentiel disruptif. D'autres technologies au potentiel disruptif sont par exemple l'intelligence artificielle (IA) ou les réseaux 5G+.

Les effets des menaces provenant du cyberespace sont très variés : ils vont des opérations à court terme visant à perturber les infrastructures critiques, telles que les attaques par déni de service distribué (Distributed-Denial-of-Service, DDoS), à l'intégration non détectée à long terme de cyberarmes – pouvant être déclenchées en cas de besoin – dans les systèmes TIC. Alors qu'un conflit mené exclusivement dans le cyberespace est

aujourd'hui considéré comme irréaliste, de telles attaques en préparation d'un conflit militaire ou dans le cadre d'engagements militaires pendant un conflit sont déjà une réalité.

Les cyberattaques ne sont toutefois pas toutes motivées par des raisons militaires, loin s'en faut. Selon la SNPC, la cybercriminalité est combattue par les autorités civiles. En revanche, il existe dans le cas du cyberespionnage aussi bien des aspects économiques que militaires. Le cyberespionnage se produit en permanence, de manière cachée et indépendamment des conflits. Cela concerne aussi bien les réseaux gouvernementaux contenant des informations classifiées que les entreprises et les institutions de recherche. Par exemple, l'infiltration des chaînes d'approvisionnement de logiciels et de matériel touche de larges pans de l'économie. De telles actions sont complexes et nécessitent beaucoup de temps de préparation de la part des cyberattaquants. C'est pourquoi l'autoprotection est une tâche permanente et importante, même en dehors des périodes de crise.

Dans le domaine de l'autoprotection dans le cyberespace, l'accent est mis sur les technologies permettant de détecter les cyberrisques à un stade précoce, d'améliorer les mesures de défense et de rechercher et valider les vulnérabilités ou les problèmes de sécurité. Les analyses manuelles de programmes potentiellement malveillants ne peuvent toutefois plus suivre le rythme de l'évolution et le nombre de vulnérabilités potentielles. Il faut donc s'attendre à des progrès importants dans l'automatisation des analyses de sécurité. Cela concerne divers aspects comme la recherche d'échantillons défectueux dans le code source et l'analyse du comportement des programmes pendant leur exécution. Les logiciels sont généralement constitués de différents composants standard. Il est donc important d'identifier les composants suspects présentant des failles de sécurité connues. Si des vulnérabilités ont été trouvées, il faut également disposer de méthodes automatisées permettant de vérifier l'exploitabilité pour des attaques, de façon à pouvoir évaluer la menace effective.

Concernant la détection précoce des cyberrisques et leur évaluation, l'accent est mis sur la sécurité des systèmes individuels, mais aussi sur la sécurité de toute la chaîne d'approvisionnement. Pour combler cette lacune en matière de capacités sur un système individuel, il doit être possible de contrôler les composants via toutes les interfaces accessibles. Par interface, on entend toute connexion et tout protocole prévus par le système pour échanger des données ou des signaux de commande. Cela s'applique autant aux logiciels qu'au matériel. Les possibilités d'échange de données ou de signaux de commande par le biais d'autres voies que les interfaces prévues constituent alors un défi. De telles possibilités supplémentaires sont regroupées sous le terme de canaux auxiliaires. Un système isolé d'Internet qui a été compromis via la chaîne d'approvisionnement peut par exemple transmettre des données à un système voisin équipé d'une caméra grâce à des clignotements générés de manière ciblée par le voyant d'activité du disque dur. Outre les nombreux canaux auxiliaires déjà connus et bien étudiés quant à leur potentiel de danger, il existe également – en particulier dans les systèmes informatiques hétérogènes composés aujourd'hui de plusieurs unités de calcul et de stockage – de nouvelles approches permettant d'utiliser des canaux auxiliaires pour lancer des attaques. Ces nouvelles approches reposent sur la possibilité d'influence mutuelle des différents éléments constitutifs. Dans le cas des canaux auxiliaires basés sur la radio, il est par exemple possible d'influencer et d'attaquer des systèmes tels que la domotique ou les systèmes de charge de véhicules électriques, qui communiquent entre eux via le réseau électrique.

Les schémas d'attaque dans le cyberespace sont de plus en plus sophistiqués. Il est donc nécessaire que les mesures de défense suivent le rythme de l'évolution des schémas d'attaque. L'accent sera mis sur l'amélioration des méthodes de détection des attaques, qui reposent généralement sur l'intelligence artificielle, et de la réponse automatique à celles-ci. Les technologies de réseau de plus en plus rapides, la virtualisation de l'infrastructure et son déplacement vers le cloud constituent ici un défi particulier. Dans de tels cas, les approches de défense traditionnelles ne fonctionnent plus que partiellement car les grandes quantités de données à traiter rapidement ne le permettent plus ou augmenteraient trop les coûts. Un autre secteur qui fait l'objet d'une attention accrue de la part des chercheurs dans le domaine des mesures de défense est celui des technologies de camouflage et de leurrage, comme la défense de cible mobile en réseau (In-Network Moving Target Defense) pour la 5G+. Pour cela, les paramètres et topologies du système sont continuellement modifiés afin de déstabiliser les cyberattaquants. Ce secteur est intéressant d'un point de vue militaire, car il est pertinent aussi bien pour l'autoprotection que pour les actions dans le CYBEEM. Grâce à l'intelligence artificielle antagoniste et à l'ac-

cès à un système de détection des attaques basé sur l'IA et utilisé par le défenseur, un attaquant peut par exemple trouver des moyens d'éviter d'être détecté. Ou, alternativement, le système peut être amené à ne pas reconnaître certains schémas d'attaque utilisés par l'attaquant, à condition que l'attaquant puisse influencer au moins partiellement les données d'entraînement pour le système utilisé par le défenseur.

Images de la situation cyber

Une image complète de la situation cyber est essentielle pour identifier et analyser en temps voulu les risques et les menaces concrètes et y réagir de manière appropriée. Parmi les éléments centraux de l'élaboration d'images de la situation cyber, nous trouvons les technologies et les méthodes permettant de recenser les cyberrisques dans les infrastructures TIC, d'échanger des données avec différents services et partenaires si possible de manière automatisée, lisible par machine et sans trop s'exposer soi-même, de collecter dans le cyberespace des renseignements d'origine sources ouvertes (ROSO) et de fusionner les informations de manière utile.

La connaissance précise de sa propre infrastructure TIC est une condition indispensable pour pouvoir identifier les cyberrisques. Tous les aspects, allant de l'application critique jusqu'à l'appareil individuel, doivent être pris en compte. En raison des technologies modernes, telles que le software-defined networking, la 5G+, l'IdO et le cloud, les infrastructures TIC sont de plus en plus dynamiques et diversifiées. Grâce à l'amélioration des méthodes et des technologies, les éléments constitutifs des infrastructures TIC pourraient à l'avenir être enregistrés de manière entièrement automatisée.

Dans le domaine de l'acquisition de données pour l'image de la situation cyber, l'échange et la coopération avec différents services et partenaires deviennent de plus en plus importants. Les défis à relever sont notamment la quantité croissante d'informations et le souhait de partager les informations de manière à ce qu'il en résulte un bénéfice maximal, sans qu'il ne soit nécessaire d'en révéler trop sur soi-même. Pour traiter de grandes quantités de données, l'accent est mis sur les technologies et les méthodes qui aident à regrouper n'importe quelles informations et à les traduire dans des formats structurés et lisibles par une machine pour en faciliter le traitement. Les progrès réalisés dans le domaine des grands modèles de langage laissent entrevoir ici des solutions inédites. En ce qui concerne l'échange d'informations, l'accent est mis sur des solutions qui garantissent que les données partagées ne contiennent pas de données dont l'échange constitue une violation de la protection des données ou qui sont problématiques d'une autre manière. Différentes technologies telles que le chiffrement homomorphe, le calcul multipartite ou le confidential computing (informatique confidentielle) ont ici le potentiel de surmonter d'autres obstacles en ce qui concerne l'aptitude pratique et de produire des solutions plus largement applicables.

Lorsqu'il s'agit d'évaluer la situation en matière de cybermenaces, les informations concernant les partenaires et notamment aussi les renseignements d'origine sources ouvertes (ROSO) collectés dans le cyberespace et accessibles au public sont hautement pertinents. Alors que de nombreuses sources de données intéressantes et méthodes associées permettant de déduire des informations utiles sont déjà connues, il existe un grand potentiel pour d'autres sources et méthodes. La quantité de données et le nombre de services et d'utilisations du cyberespace continuent de croître fortement. En raison de la forte dynamique des développements dans le cyberespace, des approches robustes sont nécessaires pour évaluer la qualité et la valeur d'usage des données ROSO et pour pouvoir les surveiller à plus long terme. Enfin, afin de rassembler toutes les informations de manière profitable, il faut des méthodes et des technologies appropriées pour fusionner les données (voir à ce sujet le chapitre 3.3.3 Science des données et image de la situation).

Traitement des données robuste et sûr

La capacité à traiter et à distribuer des données de manière robuste et sûre est essentielle pour la capacité d'action de l'armée ainsi que de l'économie et de la société, qui sont en grande partie numérisées. Pour y parvenir, il est nécessaire que les éléments constitutifs et les technologies des infrastructures TIC soient intrinsèquement robustes et sûrs, et ne dépendent pas de mesures et de technologies supplémentaires pour détecter et combattre les problèmes de sécurité. Cela peut être réalisé en utilisant des technologies pour lesquelles la sécurité et la robustesse ont été prises en compte dès leur conception ou qui ont été conçues spécifiquement pour fonctionner dans un environnement hostile. On peut observer ici plusieurs développements pertinents, comme les technologies pour les réseaux de communication qui sont robustes et sûres pour résister à des attaques telles que le détournement du trafic via des chemins de réseau pro-

blématiques ou à certains types d'attaques par déni de service.

La cryptographie et les technologies visant à réduire ce que l'on appelle la base informatique de confiance (Trusted Computing Base) comportent d'autres exemples de développements pertinents. La Trusted Computing Base désigne l'ensemble des logiciels et des matériels auxquels il faut faire confiance pour être sûr qu'un système ou une application présente les caractéristiques de sécurité attendues. Plus la Trusted Computing Base est petite, plus la surface d'attaque de l'extérieur et donc le risque d'être compromis sont réduits.
Dans le domaine du traitement sécurisé des données, il convient de mentionner en particulier les domaines de recherche découlant du développement d'ordinateurs quantiques : la cryptographie quantique et la cryptographie post-quantique. Cette dernière étudie des méthodes de chiffrement et de signature qui sont sûres même contre les agresseurs utilisant des ordinateurs quantiques. Du fait du potentiel disruptif des ordinateurs quantiques pour l'ensemble de l'Internet, il est impératif de suivre et d'étudier de près les développements dans ce domaine. Il est notamment nécessaire d'anticiper les risques concrets à temps, car une mise à niveau des systèmes existants (civils et militaires) avec la cryptographie post-quantique n'est pas anodine et il faut prévoir plusieurs années pour cela. Si des développements spectaculaires devaient avoir lieu pendant cette période, une fenêtre d'opportunité s'ouvre alors pour les attaquants.

En outre, il faut s'attendre à ce que la cryptographie fasse des progrès dans le domaine du confidential computing. Ce terme regroupe les technologies qui permettent de stocker et de traiter des données sur du matériel et des logiciels non fiables, comme dans le cloud public. Les technologies de base telles que les Trusted Execution Environments (environnements d'exécution de confiance), c'est-à-dire des environnements séparés et sécurisés pour l'exécution de programmes, ou de nouvelles fonctions de sécurité dans les processeurs modernes y contribuent tout autant que les nombreuses technologies qui s'appuient dessus. Grâce à des méthodes spéciales, il est même possible d'effectuer des calculs sur des données sensibles à travers plusieurs parties, sans que les données ne soient visibles pour des tierces parties. Cela permet l'utilisation d'applications qui était impossible jusqu'ici en raison des exigences en matière de protection des données.

En plus de ces domaines, on peut toutefois également s'attendre à des développements pertinents dans d'autres domaines, par exemple dans le domaine des systèmes d'exploitation hautement sécurisés, des technologies vérifiant les caractéristiques de sécurité des logiciels et du matériel ou encore en ce qui concerne les nouveaux protocoles de communication hautement sécurisés.

Actions dans le cyberespace

La guerre en Ukraine montre que l'utilisation de moyens d'attaque dans le cyberespace à des fins hégémoniques est déjà la norme. La perturbation des télécommunications et de l'approvisionnement en énergie civils passe aujourd'hui par des actions menées principalement dans l'espace électromagnétique, mais aussi de plus en plus dans le cyberespace. Les cyberattaques classiques font partie du répertoire, tout comme les attaques et les actions d'espionnage avec des logiciels malveillants. L'armée doit être en mesure de détecter à tout moment de telles attaques et de protéger ses propres systèmes et infrastructures. Des mesures actives peuvent également être utilisées pour se défendre contre les cyberattaques. Les moyens correspondants de l'armée sont utilisés en priorité pour l'autoprotection. Les bases légales pour le développement et l'adoption de mesures actives et de contre-mesures dans le cadre de la cyberdéfense sont régies par la loi fédérale sur le renseignement et la loi sur l'armée révisée.
En raison de l'évolution constante et rapide du monde technologique, dans lequel les systèmes TIC typiques sont renouvelés tous les cinq à six ans, le développement et l'utilisation des capacités et des outils nécessaires aux actions dans le cyberespace constituent un défi majeur. Pour compliquer les choses, un outil d'attaque peut perdre son efficacité d'un moment à l'autre, par exemple lorsqu'un logiciel malveillant est découvert par la partie adverse. En outre, la faille de sécurité utilisée peut également être corrigée délibérément par la maintenance régulière du système (comme les mises à jour), ou par hasard, suite à une modification du système dans le domaine concerné.
En ce qui concerne les outils d'attaque, on observe plusieurs tendances. L'utilisation d'ordinateurs quantiques pour mener des attaques contre des procédures cryptographiques et les progrès radicaux dans l'utilisation de l'intelligence artificielle pourraient également entraîner des changements disruptifs dans ce domaine. Pour qu'une faille puisse être utilisée pendant une attaque, il faut développer ce que l'on appelle un « exploit ». Celui-ci se compose généralement d'une séquence spécifique d'instructions et de fragments de

données ou d'un code de programme. Le développement d'exploits requiert souvent un investissement personnel très important. La situation est aggravée par le fait que la durée d'utilisation d'un tel exploit est généralement courte. C'est pourquoi un travail intensif est réalisé pour automatiser le développement d'exploits.

L'identification des vulnérabilités constitue une base essentielle pour les actions dans le cyberespace. Par conséquent, les méthodes et les technologies élaborées pour la cyberprotection peuvent également être utilisées ici et inversement. Dans le CYBEEM, il en va de même que dans toutes les autres sphères d'opération : celui qui ne connaît pas la protection et les contre-mesures d'un adversaire ne peut pas évaluer l'effet de ses moyens opérationnels. Celui qui n'est pas en mesure d'évaluer la capacité d'action de son opposant ne sait pas comment évaluer la protection de ses propres moyens.

Thèmes de recherche 2025-2028

Autoprotection CYBEEM

- Évolution des compétences technico-scientifiques pour l'autoprotection dans le CYBEEM à l'aide de technologies de sécurité pour la prévention, la détection et la correction des cyberactivités malveillantes
- Étude, développement continu et évaluation de méthodes et de technologies permettant d'automatiser l'utilisation de ses propres cyberpouvoirs
- Étude et évaluation de méthodes permettant de trouver automatiquement des vulnérabilités dans des systèmes propres et étrangers
- Suivi et évaluation de solutions de protection des systèmes dans le cyberespace basées sur l'intelligence artificielle, en mettant l'accent sur leur robustesse dans le champ d'application
- Étude de vulnérabilités dans les modèles et méthodes d'apprentissage automatique afin d'améliorer leur robustesse face aux attaques

Images de la situation cyber

- Surveillance de nouveaux vecteurs d'attaque et d'autres développements qui représentent des opportunités et des menaces extraordinaires pour la sécurité dans le cyberespace
- Développement et amélioration d'indicateurs publiquement disponibles (ROSO) et développement des connaissances permettant d'évaluer leur qualité et leur valeur d'usage
- Étude et développement continu de technologies permettant d'échanger des informations sur les cyberattaques de manière sûre et conforme à la protection des données, et évaluation de la sécurité de ces technologies

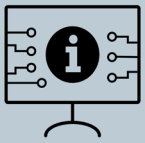
Traitement des données robuste et sûr

- Identification et développement de compétences en matière de nouvelles technologies de sécurité et de protection de la vie privée, telles que la cryptographie post-quantique, le confidential computing ou les technologies quantiques
- Étude et évaluation du potentiel des technologies d'isolation basées sur le matériel et les logiciels, par exemple pour l'utilisation de terminaux mobiles ou d'infrastructures cloud pour des travaux nécessitant différents niveaux de protection
- Étude et évaluation des technologies et protocoles de réseau de nouvelle génération en ce qui concerne les opportunités, les risques et les conditions-cadres de leur utilisation

Actions dans le cyberespace

- Élaboration de méthodes pour l'exploitation automatisée de vulnérabilités
- Étude de nouveaux vecteurs d'attaque et de leur effet, par ex. les nouveaux vecteurs d'attaque par déni de service
- Observation des normes et des points de référence internationaux pour l'évaluation de l'efficacité des vecteurs d'attaque
- Suivi des nouvelles méthodes et technologies de camouflage et de leurrage dans le cyberespace
- Développement continu de méthodes et de technologies permettant d'automatiser la procédure des cyberacteurs adverses dans les situations d'entraînement des Blue Teams
- Étude de nouvelles approches et technologies pour la défense des cybersystèmes par des actions offensives propres

3.2.3 Technologies pour garantir la supériorité de l'information



Situation de départ et problématique

Dans de nombreuses armées, les technologies modernes jouent un rôle central dans l'implémentation d'un CRCA de bout en bout et intelligent. C'est ce que montrent aussi bien les conflits conventionnels que les scénarios asymétriques qui se sont déroulés dans un passé récent. Il s'agit en premier lieu de fusionner les données des capteurs et les informations des services de renseignement, si possible en temps réel, pour obtenir une image de la situation claire et adaptée à chaque niveau, afin que les opérations puissent être menées dans un contexte de supériorité de l'information et que des effets adéquats puissent être obtenus de manière coordonnée et en temps voulu. Outre l'accélération des cycles d'instruction – de la saisie de la situation à l'analyse de l'effet obtenu – les technologies modernes permettent également une amélioration de la compréhension de la situation, car davantage de données et de sources d'information peuvent être traitées en parallèle et avec une qualité supérieure. L'association d'images numériques de la situation avec la possibilité de simulation au profit de la planification des opérations et de la donnée d'ordres dans un secteur d'engagement contribuent à une utilisation optimale des moyens à disposition. Cependant, de nouveaux défis dans la génération de la supériorité de l'information doivent être relevés dans le cadre du CRCA, par exemple en raison de nouvelles possibilités intelligentes de camouflage, de leurrage et de brouillage, ainsi qu'en raison de contre-mesures modernes dans le cyberespace et l'espace électromagnétique.

Les technologies de l'information ont une forte influence sur la société qui est continuellement exposée aux nouvelles technologies de l'information et de la communication. La génération Z, en particulier, a grandi avec les technologies numériques telles qu'Internet, les smartphones et les tablettes. La société dans son ensemble s'est adaptée aux évolutions technologiques et utilise les nouvelles technologies au quotidien. Pour la conduite des opérations militaires, il est toutefois difficile d'atteindre efficacement – avec les moyens standard actuels – un degré élevé de mise en réseau, même dans des situations exceptionnelles.

Les changements actuels conduisent à une nouvelle façon de communiquer et d'informer, qui fait que les photos, les vidéos et les informations sont immédiatement accessibles à un large public mondial. Cela accélère l'échange d'informations et suscite une demande croissante de données en ligne accessibles à tous. Les services de renseignement ont toujours utilisé des sources ouvertes et, de plus en plus, les médias sociaux pour obtenir des informations (ROSO et SOCMINT, Social Media Intelligence). Cependant, ces sources peuvent également être utilisées à des fins abusives, d'où l'importance de détecter les fausses informations. Malheureusement, les fake news et les vidéos manipulées sont de plus en plus sophistiquées.

La numérisation, l'intelligence artificielle et les big data ont considérablement évolué et ont désormais rejoint la société civile. Les smartphones utilisent depuis longtemps déjà des algorithmes intelligents pour trier les photos, reconnaître les visages, les voix et les lieux, et prédire les textes. Néanmoins, l'IA n'a pas encore pleinement réussi dans tous les domaines d'application, notamment dans les systèmes militaires. Cela est dû au grand nombre de données de référence classifiées nécessaires, à la complexité des applications et à la vulnérabilité de l'IA face aux attaques hostiles, appelées adversarial attacks (attaques adverses).

Dans le domaine militaire, on observera une certaine réticence à utiliser de nombreuses applications d'IA tant que ces dernières conduiront à des résultats qui sont des plausibilisés dans le meilleur des cas, mais qui, souvent, ne peuvent pas être expliqués dans le détail et ne sont pas compréhensibles. Cela est tout à fait compréhensible, d'autant plus que la portée des décisions peut être sensiblement différente de celle des applications civiles. Cependant, il convient aussi de noter que les décisions prises intuitivement pourraient très bien présenter un manque de traçabilité. À l'avenir, les limites de l'IA doivent être examinées de manière critique. Néanmoins, l'automatisation dans les systèmes militaires basée sur le cycle OODA (Observe, Orient, Decide, Act) et l'accélération de la collecte d'informations sont des tendances irréversibles. Il faut s'attendre à des améliorations significatives dans les années à venir.

Outre les tendances de l'IA et des big data, on observe également dans la société une tendance vers les so-

lutions intelligentes locales. Des capteurs portables, appelés wearables, mesurent les fonctions corporelles et effectuent des évaluations locales. Les appareils IdO et les réseaux IdO prennent de plus en plus d'importance. Ces appareils ne se contentent pas d'enregistrer leur environnement, mais ils traitent localement les valeurs mesurées et transmettent les résultats fortement compressés par communication mobile. Comme de nombreux appareils sont souvent connectés en réseau, on parle aussi de communication de machine à machine. L'intelligence locale, également appelée Edge Intelligence, est une tendance que l'on ne peut ignorer. Dans le domaine militaire, l'intelligence locale et les réseaux IdO suscitent également de l'intérêt. Il faut toutefois répondre à des exigences spécifiques en matière de robustesse, de sécurité, de résistance aux interférences et de résilience dans un environnement militaire, car les réseaux IdO civils ne répondent pas entièrement à ces exigences.

Reconnaissance et surveillance

Pour obtenir une supériorité de l'information, une collecte d'informations ciblée et rapide est déterminante. La reconnaissance et la surveillance sont une source importante pour déclencher le flux d'informations entre les capteurs, les décideurs et les effecteurs. Différentes sources d'information sont utilisées à cet effet, telles que le renseignement humain (HUMINT), le renseignement obtenu par l'image (IMINT), l'exploration électromagnétique (SIGINT), le renseignement par radar (RADINT), le renseignement géospatial (GEOINT), le renseignement par mesures et signatures (MASINT) et le renseignement électro-optique (VISINT). Les systèmes multi-capteurs, les méthodes d'évaluation intelligentes et la fusion des données des capteurs jouent un rôle central lors du traitement des informations. Grâce à la numérisation des données des capteurs et à l'augmentation de la puissance des processeurs, des applications en temps réel et des évaluations préalables intelligentes de haute qualité sont possibles. Ce développement permet le traitement automatisé des données des capteurs pour obtenir des informations de reconnaissance et de surveillance directement sur la plateforme d'engagement. Les plateformes peuvent ainsi être conçues pour des missions de reconnaissance et de surveillance, ce qui peut contribuer à réduire les coûts et les effectifs. L'obtention et le traitement rapides des informations ainsi que l'établissement d'images actuelles de la situation sont ainsi facilités.

Afin de garantir la supériorité de l'information dans le cadre d'une conduite des opérations en réseau, les investissements dans la recherche et le développement de technologies modernes de détection et de reconnaissance sont énormes au niveau international. Dans ce contexte, on constate également que de gros efforts sont toujours réalisés dans le domaine du combat électronique (electronic warfare). On observe ainsi de plus en plus de mesures intelligentes de leurrage et de brouillage ainsi que des contre-mesures dans l'espace électromagnétique.

La quantité et la qualité des données numériques des capteurs ont considérablement augmenté, tant dans le domaine militaire que dans le domaine civil. Dans le domaine civil, l'accent est mis en premier lieu sur le développement de capteurs bon marché à courte et moyenne portée, comme les radars pour les voitures ou les capteurs pour les smartphones. Le système de caméra est probablement le type de capteur le plus répandu aujourd'hui. L'amélioration de la résolution augmente le niveau de détail et le contenu informatif des photos, mais aussi la quantité de données et le besoin de stockage. La progression de la miniaturisation des capteurs et leur consommation d'énergie réduite contribuent à ce que les données puissent être enregistrées par n'importe qui, n'importe quand, n'importe où et sur n'importe quel support, comme des mini-drones, et à ce qu'elles communiquent entre elles (IdO). C'est pourquoi la détection des menaces que représentent les mini-drones et les micro-drones est aujourd'hui essentielle, aussi bien pour les forces de sécurité civiles que militaires. Le marché propose des systèmes de détection de drones plutôt économiques pour les entreprises de sécurité privées et des systèmes complets et sophistiqués pour les utilisateurs militaires.

La miniaturisation des satellites permet aux entreprises de proposer de nouveaux produits satellitaires à double usage, avec un contenu informatif important et une bonne résolution temporelle. Il est aujourd'hui possible d'acquérir à titre commercial des images satellites spéciales, notamment des images visuelles et radar à haute résolution de zones de conflit. Autrefois réservées aux services secrets, ces images sont désormais accessibles au public. Les médias occidentaux et les instituts de sécurité publique ont utilisé ces images pour analyser et documenter les conflits récents. Bien que la qualité des images de petits satellites ne soit pas comparable à celle des satellites espions, elles contiennent néanmoins des informations importantes. Cette évolution joue donc un rôle crucial pour tous

les acteurs impliqués dans la collecte d'informations à partir d'images satellites.

La collecte d'informations, la reconnaissance et la surveillance ne peuvent pas être réduites à de simples questions techniques. Outre la disponibilité et la mise en réseau des systèmes techniques, des facteurs tels que les caractéristiques organisationnelles et culturelles ainsi que les directives doctrinales jouent un rôle crucial dans le traitement des informations, en particulier lors d'opérations multinationales. Dans un contexte militaire, le renseignement et la surveillance sont essentiels pour obtenir des informations et acquérir une supériorité de l'information par rapport aux forces adverses.

Communication

Les systèmes de communication mettent en réseau les sources de données et d'informations avec les décideurs et les effecteurs et doivent être disponibles à tout moment. Ils constituent ainsi l'épine dorsale du système global de l'armée et permettent l'utilisation de systèmes de conduite et d'information, tant dans le domaine militaire que civil. Une transmission sûre, robuste, en temps réel et mobile de données telles que la voix, les images et le texte, sans ruptures de média involontaires, sont des conditions essentielles pour mener à bien des engagements. Les réseaux de communication hétérogènes sont d'une importance capitale lors d'engagements en réseau, car aucune technologie ne peut à elle seule répondre à toutes les exigences. L'interopérabilité entre les propres systèmes de communication et ceux des partenaires est essentielle. Les tendances de développement dans le domaine des technologies de l'information et de la communication (TIC) sont principalement déterminées par la demande de transmission de grandes quantités de données sur les marchés civils. Cela entraîne une demande accrue de bande passante, ce qui oblige les opérateurs de téléphonie mobile à étendre constamment leurs réseaux et à les équiper des dernières technologies. Actuellement, les opérateurs de télécommunications civils investissent dans le déploiement du réseau de téléphonie mobile 5G afin de créer les conditions nécessaires aux applications intelligentes dans l'économie, le secteur privé et l'administration publique. Les discussions sur les possibilités de la 6G ont également déjà commencé.

Les forces de sécurité ont des exigences spécifiques en matière de sécurité du réseau contre les défaillances et de prévention des perturbations. Dans l'environnement militaire, la robustesse des propres moyens de communication contre les actions perturbatrices dans l'espace électromagnétique est au centre des préoccupations, car cela limiterait le CRCA, aussi bien en termes de temps que de qualité. Ce durcissement des systèmes, mais aussi la protection contre l'accès non autorisé aux informations, ne sont souvent pas suffisamment pris en compte par les fournisseurs civils. Les forces de sécurité doivent donc développer leurs propres solutions spécifiques, ce qui implique des coûts plus élevés et un temps de développement plus long. Il est toutefois important de suivre les tendances et d'assurer la connectivité entre les applications de communication militaires et civiles.

La tendance à transmettre des quantités toujours plus importantes de données et d'informations, et donc à utiliser des bandes passantes toujours plus larges, va accroître la pression afin que les bandes de fréquences actuellement réservées aux applications dans le domaine de la sécurité soient rendues accessibles à un usage civil. Il s'agit donc d'utiliser le plus efficacement possible les ressources en fréquences disponibles. Grâce aux technologies radio modernes telles que la radio logicielle (SDR, Software Defined Radio) et la radio cognitive, il est possible d'adapter la forme d'onde et donc la propagation dans l'espace, la fréquence ainsi que la bande passante nécessaire à l'occupation de l'espace électromagnétique et de l'optimiser en fonction des besoins de transmission des informations. Ainsi, les réseaux pour les forces de sécurité peuvent non seulement être conçus de manière plus flexible et en même temps plus robuste, mais ils peuvent également être exploités de manière plus performante. De plus, l'intelligence artificielle permet d'optimiser le routage des données et donc le flux de données. L'exploitation de réseaux cellulaires sera également nécessaire dans le domaine militaire pour permettre la transmission de grandes quantités de données. Dans ce contexte, c'est surtout la technologie issue de la téléphonie mobile civile qui permet l'utilisation d'une puissance de calcul répartie au sein de réseaux locaux qui peuvent être reliés à l'infrastructure haute performance via des nœuds semi-mobiles. Des services générés par les bases arrières, comme la reconnaissance d'images, les services de traduction ou l'identification des systèmes adverses, deviennent ainsi disponibles sur place.

Grâce à l'augmentation des performances et à la miniaturisation, les appareils radio peuvent être utilisés de façon de plus en plus polyvalente. Les signaux radio sont numérisés et peuvent donc être traités de n'im-

porte quelle manière. Cela ouvre la possibilité d'intégrer sur la même plateforme, outre les services de communication classiques, d'autres capacités telles que la reconnaissance dans l'espace électromagnétique. À l'avenir, cela simplifiera non seulement l'intégration de différentes applications, mais générera également une augmentation massive des capacités.

Science des données et image de la situation

L'omniprésence des données dans notre société, combinée aux progrès technologiques actuels, a entraîné la génération et l'échange de données numériques à grande échelle. Ces données sont considérées comme des mines d'or, car elles permettent aux entreprises de marketing et aux entreprises Internet de créer de nouveaux modèles de revenus en optimisant les processus et de cibler les clients plus efficacement. Des algorithmes d'apprentissage automatique sont utilisés pour analyser et exploiter ces données en regroupant des profils similaires, en classant les données ou en prédisant les tendances futures.

Ce type d'exploitation des données n'est pas seulement réservé au monde civil. L'armée et d'autres institutions étatiques, notamment le Service de renseignement de la Confédération (SRC), la Centrale nationale d'alarme (CENAL) et l'Office fédéral de la police (fedpol), peuvent également utiliser des données qu'elles produisent elles-mêmes ou qu'elles ont reçues par le biais de différents canaux. On peut également observer une tendance au regroupement de données provenant de différentes sources, qu'il s'agisse de sources internes ou de sources libres. L'utilisation d'algorithmes intelligents permet de créer différents produits en fonction de la tâche opérationnelle.

Une image de la situation est un instrument qui résume en informations des messages analysés, dans le but de donner aux décideurs une image claire de la situation actuelle dans une zone d'intérêt donnée. À cet effet, il est possible d'utiliser aussi bien des sources de renseignements militaires que des sources d'informations publiques. Une image combinée de la situation permet une compréhension commune de la situation et une action coordonnée entre les différents services. Grâce à l'utilisation de l'intelligence artificielle, il est possible de générer et de consolider automatiquement de telles images de la situation pour les différentes sphères d'opération. Une image de la situation actuelle, complète, adaptée à chaque niveau et claire constitue la base de décisions de conduite fondées et joue donc un rôle clé en tant qu'instrument de conduite.

Sur le plan tactique, il est important de réagir rapidement aux menaces. Les images et les informations provenant de n'importe quelle source, comme les systèmes de reconnaissance, les drones et les satellites, doivent être analysées automatiquement et en temps réel. Dans ce contexte, les algorithmes d'IA sont d'une importance capitale pour identifier les objets, les personnes, les véhicules ou les menaces. En outre, ces algorithmes peuvent être d'une aide décisive pour l'identification et le classement d'images qui proviennent d'Internet ou de réseaux sociaux et qui contiennent des informations importantes sur des adversaires. Mais l'intelligence artificielle trouve également son utilité dans de nombreuses autres applications. Pour cela, l'IA est présente à de nombreux niveaux, que ce soit de manière centralisée, mais aussi sur des capteurs, notamment pour l'automatisation de tâches répétitives ou fastidieuses.

Les informations, qu'elles soient recueillies sur place ou à partir d'autres sources, sont souvent rédigées dans des langues étrangères, voire des dialectes. Les systèmes de traduction traditionnels ne peuvent pas être considérés comme sûrs et ne sont pas en mesure de traduire les dialectes. Pour aider les analystes, il faut mettre à leur disposition des systèmes de traduction qui tiennent compte du contexte. Là encore, les développements des systèmes de traduction automatique offriront de nouvelles possibilités d'intégrer des textes qui, jusqu'à présent, devaient être traduits par des spécialistes.

À l'avenir, on peut s'attendre à ce que de nombreux systèmes tactiques ou opérationnels reposeront sur l'intelligence artificielle. Bien que cela puisse présenter de nombreux avantages, leur utilisation comporte également des risques. Comme les modèles d'apprentissage profond (Deep Learning) deviennent de plus en plus complexes, il n'est plus possible d'interpréter ou de justifier leurs décisions, ce qui signifie que la traçabilité n'est généralement plus assurée. Cela peut poser un problème éthique, notamment pour les applications de contrôle d'effecteurs. Il est tout à fait possible d'influencer et donc d'attaquer des algorithmes d'apprentissage profond, par exemple en utilisant des ensembles de données d'entraînement incomplets lors de l'optimisation d'un réseau neuronal et en empêchant ainsi la reconnaissance de certains modèles ou en manipulant la fonction cible. À l'avenir, il sera nécessaire de prendre en compte les aspects de sécurité lors de l'utilisation de l'intelligence artificielle et de s'assurer qu'elle présente une protection robuste

contre les attaques, comme tout autre système informatique.

Thèmes de recherche 2025-2028

La surveillance de l'espace aérien de demain

- Développement de nouvelles approches et méthodes pour des systèmes radars cognitifs, multifonctionnels et multistatiques
- Étude de l'influence d'environnements complexes, tels que les éoliennes, les parcs photovoltaïques ou les environnements urbains, sur la détection de cibles radar et détermination de contre-mesures en cas de perturbations
- Évaluation des défis et des opportunités liés à la combinaison d'applications radar et d'applications de communication
- Étude des technologies de détection, de suivi et d'identification de drones et d'essaims de drones dans des environnements complexes, basées sur des multi-capteurs et des multi-plateformes
- Étude de procédés pour l'utilisation d'émetteurs de communication en tant que balises pour les applications de radars passifs

Renseignement par imagerie

- Évaluation du potentiel et étude de la technologie des capteurs hyperspectraux, tant pour le renseignement par imagerie à grande échelle que pour le renseignement portant sur un petit périmètre
- Évaluation et étude de nouvelles options et tendances concernant le renseignement par imagerie indépendant des conditions météorologiques au moyen de radars à synthèse d'ouverture (RSO) sur des drones, des avions pilotés et des satellites
- Développement et évaluation de nouvelles méthodes de camouflage adaptatif
- Évaluation de méthodes avec l'intelligence artificielle pour la détection de mesures de camouflage dans le spectre visuel et infrarouge
- Étude de nouvelles approches pour la génération de scènes 3D sur la base de capteurs radar et électro-optiques
- Examen de l'influence de la météo et de la saison sur les modèles de reconnaissance d'objets

Futurs capteurs de reconnaissance

- Veille technologique dans le domaine des capteurs quantiques, concernant en particulier l'imagerie quantique basée sur des lasers et des détecteurs de photons spéciaux
- Suivi des technologies de capteurs afin de détecter les objets même lorsqu'ils ne sont pas directement visibles
- Développement continu et évaluation de méthodes et de capteurs pour la détection de cibles en mouvement
- Étude de développements dans le domaine de l'IdO, en particulier par rapport à leur potentiel pour les capteurs distribués et peu gourmands en énergie avec une intelligence locale
- Développement continu de capteurs et de méthodes de détection des risques biologiques, chimiques, nucléaires et radiologiques

Réseaux de communication intégrés

- Développement et implémentation de modèles de simulation de réseaux de communication pour l'évaluation des limites de performance
- Étude des procédés de radio logicielle pour les formes d'ondes complexes modernes et les approches de communication cognitives
- Veille technologique sur les technologies de réseau IdO et élaboration de cas d'application et de démonstrateurs pour l'armée
- Amélioration de l'efficacité spectrale et spatiale des systèmes radio grâce à des systèmes d'antennes intelligents
- Évaluation des progrès technologiques dans le traitement et la génération de signaux photoniques et développement de démonstrateurs pour les applications radar et les applications de communication
- Développement et évaluation de méthodes de synchronisation temporelle dans les réseaux de capteurs afin de réduire la dépendance vis-à-vis des systèmes de navigation par satellite
- Amélioration et développement continu de procédés de combat électronique pour la reconnaissance et l'effet dans l'espace électromagnétique

Boucle capteur-effecteur

- Amélioration de l'automatisation de la reconnaissance et de l'évaluation de la situation dans la boucle OODA afin de disposer plus rapidement de bases de décision
- Développement de concepts d'intégration de la simulation pour l'aide à la décision en tenant compte des facteurs humains
- Clarification des questions éthiques liées à l'utilisation de boucles capteurs-effecteurs automatisées

- Intégration de systèmes command and control (C2) avec des approches de jeu de guerre pour l'entraînement et les tests dans les troupes

Science des données et Intelligence artificielle pour la représentation d'images de la situation

- Étude et optimisation d'algorithmes permettant de fusionner des données multimodales pour l'établissement d'images de la situation
- Développement d'algorithmes pour des tâches de reconnaissance de texte et de traduction
- Identification et vérification de sources de données open source et dark web et développement d'algorithmes permettant la fusion de données afin d'établir une image de la situation
- Évaluation et développement d'architectures Big Data pour différents types de données et différentes applications
- Étude et évaluation de solutions de cloud hybride pour répartir le stockage de manière dynamique
- Étude de mécanismes de protection de la vie privée pour distribuer automatiquement les données et les algorithmes en fonction de leur classification, soit localement soit dans l'infrastructure cloud

Supériorité de l'information et intelligence artificielle

- Développement des compétences nécessaires pour vérifier automatiquement la robustesse des modèles d'apprentissage automatique
- Développement de critères pour l'évaluation des limites et de la sécurité des systèmes basés sur l'IA
- Étude de méthodes permettant d'expliquer différents modèles d'apprentissage automatique
- Identification des défis éthiques liés à l'utilisation de l'intelligence artificielle
- Identification et suivi des développements futurs et des applications potentielles de modèles génératifs, de l'apprentissage zero-shot (Zero-Shot Learning) et des grands modèles de langage (GPT)

3.3 Intégration de la technologie aux plateformes

3.3.1 Autonomie et robotique

Situation de départ et problématique

Au niveau international, la recherche dans le domaine de la robotique ou des systèmes sans occupants est devenue une priorité, et ce dans le secteur civil comme dans le secteur militaire. Les objectifs principaux de l'utilisation de la robotique sont multiples. Ils consistent principalement à accroître l'efficacité et l'efficience dans l'exécution de certaines tâches, à soulager les personnes des tâches répétitives, ennuyeuses et fatigantes et à tenir éloignées les personnes des environnements dangereux et menaçants. Les robots peuvent ainsi servir à augmenter la productivité et la qualité du travail, mais aussi à protéger des vies. Le spectre d'utilisation correspondant est très large et comprend presque toutes les sphères d'opération. Les aéronefs sans occupants peuvent par exemple être utilisés pour la reconnaissance, la surveillance ou l'aide à la communication, et les véhicules au sol pour le sauvetage, l'évacuation ou la logistique. Mais il est également possible de trouver des tâches utiles pour les futurs robots dans les domaines de la formation, de l'entretien et de la maintenance.

Dans le domaine des systèmes sans occupants, la rapidité des développements performants repose généralement sur des compétences système qui permettent d'intégrer habilement des composants commerciaux prêts à l'emploi (COTS) et des composants militaires prêts à l'emploi (MOTS). La mise à disposition de systèmes autonomes performants dépend essentiellement des progrès réalisés dans les technologies dites « facilitatrices », telles que les technologies de capteurs, de calculateur ou de communication, ou des progrès réalisés dans les domaines de la propulsion, de la navigation, du stockage de l'énergie ou des interfaces homme-machine et machine-machine. Ce sont surtout les progrès réalisés ces dernières années par l'intelligence artificielle qui nous montrent que les robots peuvent être utilisés de manière de plus en plus indépendante de l'homme pour des tâches et dans des environnements de plus en plus difficiles.

Néanmoins, l'utilisation de systèmes sans occupants ne dépend pas uniquement d'aspects techniques, mais également d'une multitude de facteurs sociaux, législatifs et éthiques, tels que la confiance accordée à ces systèmes et l'acceptation de ces derniers par les utilisateurs et la société, l'évolution de la situation juridique nationale et internationale ou les débats éthiques et moraux.

Les autorités civiles et militaires ainsi que les organisations chargées de missions de sécurité accordent de plus en plus d'importance à la robotique. Dans les conflits armés, les drones et les robots occupent une place de plus en plus importante, tant chez les acteurs étatiques que non étatiques. Les effectifs limités de soldats et de spécialistes formés à grands frais ainsi que la pression exercée par les valeurs de notre société exigent des opérations militaires dont les risques sont largement minimisés. L'utilisation de systèmes sans occupants est donc une évidence. Jusqu'à présent, les plateformes sans occupants étaient généralement déployées à distance, depuis une position arrière, et nécessitaient des ressources humaines importantes. Cependant, les progrès réalisés dans le cas des systèmes embarqués avec des algorithmes d'IA permettent une autonomie croissante des plateformes sans occupants. En outre, les nouvelles capacités d'effectuer des missions de longue durée permettent d'élargir considérablement les types de missions possibles pour ces systèmes autonomes. Il est donc prévisible que les systèmes sans occupants seront utilisés comme plateformes dans

un très large éventail de capacités opérationnelles, notamment partout où des soldats ou des civils devraient être exposés à de très grands dangers ou lorsque la fatigue de l'équipage deviendrait un problème en raison de la durée d'une mission. Néanmoins, trois conditions sont nécessaires pour une prestation d'engagement optimale. Premièrement, il faut des interfaces utilisateur intuitives qui rendent la tâche plus facile pour l'opérateur. Deuxièmement, il faut garantir à la fois une large interopérabilité technique avec l'environnement système existant et une intégration sans faille dans les processus des forces de sécurité. Finalement, afin d'exploiter de nouveaux aspects tactiques dans des concepts d'engagement opérationnels, il est impératif d'étayer la collaboration entre l'homme et la machine sur le plan doctrinal.

Les progrès technologiques des systèmes sans occupants sont un avantage pour les opérations de reconnaissance et de surveillance, mais se révèlent être un inconvénient du point de vue de l'appréciation de la menace. Un exemple typique qui a souvent été sous-estimé est celui des micro-drones et des mini-drones low-tech. Leur grande disponibilité, leur coût relativement faible, les obstacles logistiques minimes et leur fonctionnement sans infrastructure coûteuse rendent leur utilisation probable même dans des scénarios asymétriques ou à des niveaux d'escalade inférieurs au seuil des hostilités. Dans ce contexte, leur utilisation par des forces adverses nécessite la mise en place de mesures de protection et de contre-mesures afin de protéger les soldats, les systèmes coûteux et les infrastructures critiques. Il convient donc d'approfondir la réflexion sur la manière de traiter les systèmes adverses armés ou non armés. En raison de leur potentiel, les systèmes sans occupants représentent différentes menaces dont les conséquences ne peuvent pas encore être évaluées de manière définitive à l'heure actuelle. À l'avenir, les forces de sécurité seront donc confrontées à des défis majeurs qui nécessiteront en partie un changement de mentalité.

Ces dernières années, ce sont surtout les marchés civils qui ont déterminé le développement des drones et des robots. Ils voient dans ces systèmes une possibilité de fournir des services d'un nouveau genre ou d'optimiser des services existants. Ainsi, les premiers taxis urbains autonomes sont proposés aux personnes, des drones autonomes transportent des colis et des marchandises ou inspectent et surveillent des installations industrielles. Des plateformes volantes pourront se déplacer même à des altitudes plus importantes des espaces aériens, et ce grâce à des conditions favorables et à des réglementations plus souples, et elles pourront être utilisées pour remplacer à un prix avantageux des satellites dans la stratosphère. La mise en réseau de plusieurs plateformes à haute altitude de ce type (PHA) permettrait par exemple de mettre rapidement en place, même dans des régions à faible infrastructure et difficiles d'accès, des réseaux de communication et de les exploiter sur une période prolongée.

L'utilisation de systèmes aériens militaires sans occupants des classes HALE et MALE dans des espaces aériens spécialement délimités n'est pas nouvelle. En revanche, ce qui est nouveau, c'est de les intégrer avec une autonomie accrue dans les espaces aériens à usage civil, comme ce sera également le cas à l'avenir dans l'aviation commerciale. En effet, la militarisation des micro-drones et des mini-drones a également déjà commencé et les développements futurs ne sont qu'une question de temps. Les résultats de la recherche dans le domaine des drones de combat sont un parfait exemple de la manière dont les développements technologiques du secteur civil sont utilisés pour améliorer les performances des systèmes militaires. La progression de la miniaturisation des composants électroniques et l'augmentation des performances des propulsions se traduisent par une plus grande agilité, des temps d'utilisation plus longs et une plus grande autonomie. Il est prévisible que l'on assiste à des engagements mixtes d'hommes et de machines, lors desquels, dans une version simplifiée, le copilote d'un hélicoptère pilote un drone. L'arrivée des drones à usage unique hautement automatisés, appelés munitions rôdeuses, pour une action précise à moyenne ou grande distance, a également augmenté de manière significative.
Comme pour les systèmes aériens sans occupants, ce sont les établissements de recherche et les marchés civils qui sont les moteurs de la mobilité autonome au sol. Aujourd'hui déjà, les systèmes d'assistance à la conduite préfigurent les futurs systèmes autonomes sur la route. Bien que certains véhicules routiers autonomes soient déjà homologués à titre d'essai, il ne faut pas s'attendre à un déploiement à grande échelle avant que les aspects juridiques ne soient clarifiés. Les véhicules routiers sans conducteur peuvent être utiles aux forces armées, mais les exigences militaires posent des défis supplémentaires. Ainsi, les routes peuvent être bloquées avec des obstacles ou détruites, et l'utilisation de capteurs peut être détectée ou perturbée par des contre-mesures électroniques de l'adversaire. Le durcissement militaire de systèmes terrestres auto-

nomes entraîne des surcoûts considérables et des retards lors du déploiement.

Dans le domaine militaire, les véhicules au sol sans occupants offrent la possibilité de réduire l'exposition des forces de sécurité aux dangers, par exemple pour la neutralisation de bombes et de munitions, la détection de mines et le déminage, la reconnaissance dans les zones urbaines et dans les espaces non directement visibles, le transport de blessés et de biens de soutien dans des zones dangereuses et la reconnaissance dans des zones contaminées par des agents NBC. Au final, il est clair que la mobilité au sol va encore faire de très grands progrès, surtout dans deux domaines principaux. Le premier concerne le mode de déplacement. Ainsi, les concepts classiques d'entraînement par roues et par chenilles feront l'objet d'une évolution et ils seront complétés par des entraînements hybrides ou électriques et de nouveaux algorithmes de régulation. Ces nouvelles technologies se traduisent par des avantages tactiques, par exemple en réduisant la signature acoustique ou en augmentant l'aptitude au tout terrain. Le deuxième domaine concerne les nouveaux concepts d'entraînement, inspirés par exemple par la nature. En effet, le déplacement sur les jambes a énormément évolué ces dernières années, supplantant les concepts traditionnels des petits véhicules de moins de 50 kg équipés de roues ou de chenilles, en particulier dans des environnements naturels ou artificiels peu praticables, que ce soit en surface ou en souterrain.

Thèmes de recherche 2025-2028

Véhicules sans occupants

- Étude des possibilités techniques d'utilisation de véhicules sans occupants dans les différentes sphères d'opération, en priorité dans les sphères air et sol
- Mise en évidence du potentiel des nouveaux concepts de déplacement dans les airs, au sol et dans l'eau
- Développement des compétences nécessaires pour évaluer l'influence d'un champ de bataille moderne sur l'utilisation des véhicules sans occupants, par exemple pour évaluer les méthodes de localisation dans un environnement à GNSS dégradé
- Étude de charges utiles pertinentes pour les missions et intégration de ces charges utiles dans des plateformes sans occupants
- Estimation de l'impact des développements dans les technologies clés en ce qui concerne l'extension des capacités des systèmes sans occupants

Homme-machine et autonomie

- Identification des possibilités d'interaction optimale et de travail en équipe entre les personnes et les véhicules sans occupants
- Étude de nouvelles interfaces utilisateur, par exemple par le biais de la réalité augmentée, et mise en évidence de leurs avantages et inconvénients
- Étude de différents aspects dans les systèmes multi-robots, de la coopération et la collaboration jusqu'à l'essaimage et à l'interopérabilité
- Étude de l'utilisation de l'intelligence artificielle pour optimiser l'autonomie et les capacités

Intégration dans l'application militaire

- Mise en évidence des possibilités ainsi que des opportunités et des dangers engendrés par l'utilisation militaire future de véhicules sans occupants
- Étude des défis posés par l'utilisation de véhicules sans occupants, et ce de la situation normale jusqu'au conflit moderne de haute intensité
- Mise en évidence des possibilités permettant de faire face aux nouvelles formes de menaces posées par les véhicules sans occupants
- Étude de contre-contre-mesures, par exemple concernant la manière de procéder dans un environnement perturbé électromagnétiquement
- Analyse de l'évolution de la technologie et du marché dans le domaine de la robotique et des implications pour les forces armées
- Observation et évaluation du développement de systèmes d'armes autonomes létaux
- Prise en compte des questions éthiques et juridiques liées aux systèmes d'armes autonomes
- Prise en compte de l'environnement non technique afin d'identifier les opportunités et les risques pour la Suisse aux niveaux politique, militaro-stratégique et opérationnel

3.3.2 Technologies spatiales et alternatives

Situation de départ et problématique

Les applications spatiales font partie du quotidien d'une nation industrielle performante comme la Suisse. Différentes applications, telles que les prévisions météorologiques, la communication mondiale et la mise en réseau numérique, la gestion des réseaux de transport et d'énergie, la surveillance du climat et de l'environnement ou l'orientation avec un smartphone dans un lieu inconnu, sont basées sur les données des satellites se trouvant dans l'espace exoatmosphérique. Les satellites offrent la possibilité unique d'observer régulièrement et en haute résolution l'ensemble du globe terrestre et d'acquérir ainsi de nouvelles connaissances. Les données satellites servent de bases de décision dans divers domaines tels que les transports, l'agriculture, l'environnement, la sécurité et la défense.

Au début de l'ère spatiale, seules les grandes puissances pouvaient être actives dans l'espace exoatmosphérique. Aujourd'hui, grâce à des coûts de production et de lancement plus avantageux, de plus en plus d'États peuvent s'engager dans l'espace exoatmosphérique et développer et exploiter leurs propres satellites. Outre les États, il existe cependant également de nombreuses entreprises privées qui contribuent à la poursuite de l'exploitation de l'espace exoatmosphérique. La commercialisation se poursuit dans différents secteurs, les télécommunications ainsi que la reconnaissance par imagerie et la reconnaissance électronique étant les plus avancées à ce jour. Cette évolution se traduit par un nombre croissant de lancements et un nombre plus élevé de satellites. Des satellites toujours plus petits et de moins en moins chers ouvrent des possibilités nouvelles et insoupçonnées jusqu'à présent, comme la mise en place de méga-constellations composées de centaines, voire de milliers de plateformes pour la couverture mondiale des communications ou encore pour l'observation en haute résolution de la terre, et ce quasiment en temps réel. Iridium, Starlink, Oneweb, Planet, Blacksky, Capella, Iceye, Umbra, Hawkeye, Spire ou Kleos sont quelques exemples de ces constellations ou méga-constellations.

Cette évolution a incité la Suisse à formuler une nouvelle politique spatiale et même à élaborer une législation spatiale qui s'appuie sur des accords internationaux. L'objectif est de garantir que les entreprises et les institutions suisses disposent à l'avenir des bases nécessaires pour lancer des projets spatiaux ou pour y participer. L'accès simplifié à l'espace exoatmosphérique est pertinent du point de vue de la politique de sécurité, tant en termes d'opportunités que de risques potentiels. Le vol spatial a toujours été motivé et marqué par des intérêts militaires, mais ces dernières années, on a pu observer une militarisation croissante de l'espace exoatmosphérique. L'espace exoatmosphérique est une sphère d'opération de plus en plus décisive pour les forces armées modernes. C'est pourquoi certaines nations mettent en place leurs propres commandos spatiaux. L'utilisation de plateformes spatiales sert à mettre en œuvre d'autres moyens d'action ou de rendre tout simplement possible et de soutenir leur mise en œuvre. La militarisation de l'espace exoatmosphérique donne la possibilité de mener des actions militaires en orbite. L'espace exoatmosphérique pourrait ainsi passer du statut d'espace purement fonctionnel en tant que facilitateur à celui d'espace de déroulement de conflits. Plusieurs États ont créé des corps d'armée spécifiques et des structures de commandement correspondantes. L'OTAN a également déclaré l'espace exoatmosphérique comme sphère d'opération. Les capacités militaires développées permettent des actions potentiellement hostiles sur des cibles dans l'espace exoatmosphérique ou sur Terre, par exemple le lancement de satellites ou des cyberattaques. Dans les années à venir, l'espace exoatmosphérique devrait rester un théâtre de militarisation accrue et de comportements conflictuels.

En raison de la numérisation et de la mise en réseau croissante, les forces armées dépendront encore plus à l'avenir de capacités spatiales. L'utilisation diversifiée et quotidienne de données et de services provenant de l'espace exoatmosphérique accroît la dépendance vis-à-vis des infrastructures spatiales. Cela augmente la vulnérabilité de ces infrastructures aux pannes ou aux dégradations. Les satellites sont d'ores et déjà indispensables à de nombreuses applications civiles et militaires et constituent eux-mêmes des infrastructures critiques. C'est pourquoi il est non seulement nécessaire de protéger les satellites contre les cyberattaques, mais il doit également être possible à l'avenir de pouvoir les protéger de manière accrue contre les effets cinétiques et électromagnétiques, notamment contre les tempêtes solaires.

L'importance de l'espace exoatmosphérique est particulièrement pertinente pour les acteurs suisses chargés de la mise en œuvre de missions liées à la politique de sécurité. On mise pour cela sur les services de pays tiers, d'organisations ou de prestataires commerciaux. Cependant, dans le contexte de la politique de sécurité, la Suisse, en tant qu'État, n'exploite toujours pas de satellites propres à ce jour. Depuis les débuts du vol spatial en Europe, la Suisse, en tant que membre de l'Agence spatiale européenne (ESA), s'engage dans les programmes de satellites de cette dernière tout en étant également impliquée dans d'autres programmes spatiaux nationaux via des prises de participation. En outre, certains fournisseurs suisses exploitent des petits satellites dans le cadre de services commerciaux et scientifiques.

L'armée suisse est également tributaire de prestations spatiales pour accomplir ses missions, qui se présentent notamment sous la forme de contributions à la recherche de renseignements, à l'aide au commandement, à la navigation de précision et à la synchronisation de ses systèmes. Actuellement, on utilise principalement les offres de pays tiers, d'organisations ou de prestataires commerciaux pour la reconnaissance et la communication. Toutefois, l'accès à de telles informations pourrait être limité ou interdit en cas de crise ou de conflit. Ces dépendances représentent un risque pour la politique de sécurité. Afin de protéger suffisamment les opérations militaires contre la reconnaissance depuis l'espace exoatmosphérique, il est de plus en plus nécessaire de disposer d'une « image de la situation spatiale » qui tienne compte des trajectoires de survol et des capacités de reconnaissance des satellites. Enfin, l'enregistrement de la situation spatiale est un moyen permettant d'évaluer dans quelle mesure les performances des systèmes de satellites restent disponibles lorsque ceux-ci entrent en collision avec des débris, subissent des interférences ou sont même détruits par des adversaires ou sont exposés à des vents solaires accrus.

Aujourd'hui, tant l'État que le secteur privé travaillent au développement de systèmes de transport spatial réutilisables afin de réduire les coûts. L'avenir nous dira si la fiabilité de tels systèmes peut être améliorée au point de gagner la confiance des clients. Grâce à la miniaturisation des composants, il est d'ores et déjà possible de construire des satellites beaucoup plus petits. Cela permet d'une part de réduire nettement les coûts des satellites et d'autre part de lancer simultanément un nombre beaucoup plus important de satellites dans le cadre du concept rideshare, ce qui réduit encore les coûts d'accès à l'espace exoatmosphérique. Ces dernières années, la réduction des coûts et la meilleure disponibilité des systèmes de transport spatial ont permis la mise en place de grandes constellations. Celles-ci sont principalement utilisées pour les communications par satellite, pour la reconnaissance électronique ainsi que pour l'observation de la Terre. C'est en particulier dans le cas de la reconnaissance et de la surveillance que le taux de survol d'une zone cible donnée augmente avec la taille de la constellation. En cas de défaillance d'un seul satellite, cela permet ainsi d'augmenter aussi bien le volume de données collectées ou transférables que la robustesse du système. Grâce à la communication inter-satellite à large bande et à un réseau de stations au sol, il est possible de transmettre toutes les données en temps réel à une seule station terrestre. À cet effet, la communication optique par liaison laser est de plus en plus utilisée. Celle-ci permet, outre la transmission chiffrée de données, la distribution de clés quantiques. Aujourd'hui déjà, les premières grandes constellations recouvrent intégralement la Terre d'un réseau de communication par satellite. De cette manière, des connexions à large bande peuvent être offertes en tout point du globe, y compris au-dessus des océans. Pour préparer des constellations et les maintenir stables par la suite, les différents satellites doivent être manœuvrables. Pour cela, on utilise de plus en plus des propulsions électriques qui permettent surtout aux petits satellites d'effectuer des manœuvres actives et d'augmenter ainsi leur durée d'utilisation. La manœuvrabilité permet en outre à un satellite, à la fin d'une mission opérationnelle, d'être dirigé de manière ciblée vers l'atmosphère terrestre ou vers une orbite de rebut, ou encore d'effectuer des manœuvres d'évitement pour éviter une éventuelle collision avec des débris spatiaux. Pour de telles manœuvres autonomes, différents capteurs sont utilisés à bord du satellite et des décisions autonomes sont prises grâce à l'intelligence artificielle pour contrôler sa position. On peut s'attendre à ce que certains satellites ou constellations soient à l'avenir conçus de manière multifonctionnelle ou reconfigurable, c'est-à-dire qu'ils emportent en tant que charge utile plusieurs capteurs différents et des éléments de communication pouvant être utilisés en fonction des besoins.

Ces tendances génèrent d'énormes quantités de données que les analystes ne peuvent plus gérer facilement et à la vitesse nécessaire. Une évaluation proche du capteur à bord du satellite, la reconnaissance de signatures ou d'objets à l'aide de l'intelligence artifi-

cielle et l'identification automatisée des changements détectés au moyen d'une banque de données complète constituent la base des informations et des produits de services actuels par satellite destinés aux entreprises et aux autorités. L'utilisation de micro-satellites et de l'intelligence artificielle permettra également à l'avenir d'appliquer des concepts de formation et d'essaimage, dans lesquels un grand nombre de satellites seront utilisés dans différentes configurations et en fonctionnement autonome. Dans de tels concepts, les méthodes de la fabrication spatiale avancée (Advanced Space Manufacturing) (impression 3D dans l'espace exoatmosphérique) peuvent également aider à produire des pièces ou des composants de micro-satellites directement dans l'espace exoatmosphérique. Ces dernières années, le nombre de satellites lancés a fait un bond en avant pour atteindre plus de 2000 lancements par an, et la tendance laisse entrevoir des cadences de lancement encore plus élevées. Cela ne fera qu'aggraver le problème des débris spatiaux si l'on ne veille pas à ce que les satellites en fin de vie se consument suite à une rentrée atmosphérique ciblée.

En raison des développements techniques et commerciaux dans l'espace exoatmosphérique, on peut observer que même les petits États sont en mesure d'exploiter, à un coût raisonnable, des satellites de reconnaissance avec une bonne résolution spatiale, voire des petites constellations. Cela peut représenter une opportunité pour la Suisse, mais aussi un danger. Il sera également possible pour des organisations ou des États adverses, moyennant un budget modéré, de combattre d'autres satellites et de perturber ainsi la navigation GNSS ou d'interrompre les liaisons de communication. Il faut s'attendre à ce que la Suisse soit exposée à une surveillance quasi-permanente depuis l'espace exoatmosphérique, même si, par rapport aux satellites de reconnaissance optique, une couverture nuageuse d'environ 60 % et le cycle jour/nuit continueront à offrir une certaine protection à l'avenir. La situation est différente pour les capteurs radar RSO à imagerie, contre lesquels il faudrait mettre en place une protection par des contre-mesures électroniques. Dans tous les cas, les mouvements de troupes, les activités sur les aérodromes ou les déplacements de systèmes d'armes pourraient être suivis quasiment en temps réel. Si l'exploration par satellite est aujourd'hui surtout importante en tant que moyen de reconnaissance stratégique, elle sera également de plus en plus utilisée à l'avenir à des fins tactiques et opérationnelles. Pour la capacité de réaction accélérée, l'évolution va également dans le sens d'un transfert réactif de satellites afin d'établir le plus rapidement possible des capacités dans l'espace exoatmosphérique en cas de besoin ou de les remplacer en cas de défaillance. La baisse des coûts de construction, d'exploitation et de lancement des satellites ainsi que l'accès nettement facilité à l'espace exoatmosphérique ont également incité la Suisse à déterminer si les prestations fournies depuis l'espace pouvaient être couvertes, du moins en partie, par un programme national. Cela garantirait une certaine indépendance vis-à-vis de tiers en cas de crise ou de conflit. Ces réflexions ont été décrites en détail dans le concept de base de la sphère d'opération Espace exoatmosphérique, et dans le document de base Espace exoatmosphérique.

Thèmes de recherche 2025-2028

Image de la situation spatiale

- Développement de méthodes de synthèse et d'analyse de données de capteurs publiques et propres pour la représentation d'une image autonome de la situation
- Élaboration de technologies de suivi terrestre de satellites et mise en place de démonstrateurs
- Amélioration des procédures de surveillance des rampes de lancement
- Prise en compte de la météo spatiale en ce qui concerne la disponibilité des services basés sur les satellites

Applications spatiales et alternatives

- Suivi systématique de la technologie et du marché pour les applications spatiales
- Suivi des capacités et des technologies utilisées par les commandos de l'espace exoatmosphérique étrangers
- Étude des possibilités d'utilisation et des limites, et évaluation de la disponibilité, de la fiabilité et de la sécurité des constellations de satellites pour la communication
- Réalisation d'études de faisabilité afin d'évaluer les possibilités et les limites des constellations de satellites pour la reconnaissance d'images et de signaux
- Mise en évidence d'alternatives possibles pour la navigation et la synchronisation par satellite
- Développement de méthodes pour le traitement autonome et intelligent des données à bord d'un satellite afin d'accélérer la collecte d'informations

Compétences en matière de satellites et de missions

- Réalisation d'études technologiques pour le développement et l'utilisation de petits satellites
- Élaboration de bases pour la mise en place de stations au sol et pour l'exploitation d'un centre de contrôle de mission
- Évaluation de concepts pour l'utilisation réactive de satellites (Responsive Space)
- Création de bases technologiques pour l'utilisation de plateformes satellitaires flexibles et de charges utiles
- Promotion de l'écosystème Espace Suisse et mise en place de partenariats stratégiques

Protection et contre-mesures dans l'espace exoatmosphérique

- Élaboration et vérification de concepts pour le chiffrement de bout en bout des missions de satellite
- Développement continu de méthodes de protection active et passive contre la reconnaissance spatiale ennemie
- Réalisation d'analyses de risques lors de l'utilisation de services depuis l'espace exoatmosphérique
- Élaboration de modèles de coopération au niveau militaire, civil et international

3.4 Thèmes transversaux

3.4.1 Approvisionnement énergétique durable et autarcique

Situation de départ et problématique

Depuis quelques années, les thèmes du changement climatique et de l'approvisionnement énergétique durable font l'objet d'une grande attention de la part de la politique et de la société. La transition énergétique, c'est-à-dire le passage d'une utilisation non durable des énergies fossiles et de l'énergie nucléaire à un approvisionnement énergétique durable au moyen d'énergies renouvelables, pose de grands défis à l'approvisionnement énergétique civil et militaire. En 2015, la Suisse a signé l'accord de Paris sur le climat avec pour objectif de limiter le réchauffement climatique à moins de 2 degrés Celsius par rapport à l'ère préindustrielle, si possible à 1,5 degré Celsius au maximum, et de réduire d'ici 2030 les émissions de CO2 de 50 % par rapport à 1990. En outre, la loi sur le climat et l'innovation, approuvée par le peuple en 2023, a fixé comme objectif que la Suisse atteigne la neutralité climatique d'ici 2050. Comme les émissions de CO2 ne peuvent pas être totalement évitées, l'objectif de zéro net requiert également des solutions pour éliminer le CO2 de l'atmosphère et le stocker durablement.

Le DDPS, en tant que plus grand Département, est un gros consommateur d'énergie et doit, d'ici 2030, réduire ses émissions de CO2 d'au moins 40 % par rapport à 2001. En 2021, le DDPS émettait près de 200 000 tonnes de CO2 par an. Environ 47 % de ces émissions provenaient de l'aviation, 24 % du trafic routier, 20 % de l'immobilier, 7 % des déplacements de militaires et 2 % de l'utilisation de l'électricité. Le Groupement Défense est responsable d'environ 98 % des émissions de CO2 du DDPS. Les 2 % restants sont le fait des autres offices fédéraux du Département. Selon le plan d'action Énergie et climat, le DDPS a une vision claire : « D'ici 2050, le DDPS atteint la neutralité carbone (zéro émission nette). Le département couvre ses besoins en privilégiant les sources d'énergie renouvelables et vise l'autosuffisance énergétique. » Quatre grands axes ont été définis à cet effet :

- diminuer la part des énergies fossiles et favoriser leur substitution ;
- développer les énergies renouvelables et la production autonome ;
- augmenter les capacités de stockage ;
- 4encourager l'innovation.

Du point de vue de l'Armée suisse, outre la réduction des émissions de CO2, l'objectif d'un approvisionnement énergétique autarcique est également un moteur important dans la discussion sur une utilisation durable de l'énergie. La mise en réseau et la numérisation croissantes augmentent les besoins énergétiques, et les systèmes TIC en particulier sont très dépendants d'un approvisionnement en énergie fiable. La sécurité énergétique constitue donc un talon d'Achille ; elle ne doit pas être négligée mais doit au contraire être assurée en toutes circonstances. Les technologies de production et de stockage durables de l'énergie ont le potentiel d'être utilisées dans une large mesure localement et de façon autarcique. Cela ouvre la possibilité d'exploiter des sites critiques de l'armée indépendamment des fournisseurs d'énergie civils et de contribuer ainsi de manière essentielle à la capacité à durer en situation de crise.

Les dépenses publiques pour la recherche énergétique en Suisse ont fortement augmenté ces dernières années et se situent actuellement aux alentours de CHF 400 millions par an. Cette recherche couvre tout le spectre de la thématique de l'énergie, tout en

étant fortement axée sur les énergies renouvelables et l'utilisation efficace de l'énergie. Les connaissances acquises dans le cadre de la recherche civile peuvent bien entendu également être utilisées pour des applications dans un environnement militaire. Pour la production d'énergie, par exemple, les technologies sont fondamentalement les mêmes. Néanmoins, il y a aussi des aspects qui ne sont pas étudiés dans la recherche civile. Les systèmes militaires sont souvent soumis à des exigences accrues en matière de fiabilité et de capacité opérationnelle. Le défi réside dans le transfert des connaissances de la recherche civile vers le contexte militaire et dans la possibilité de les faire évoluer.

La consommation de carburant des Forces aériennes et des Forces terrestres est responsable de la majeure partie des émissions de CO2 du DDPS. Les véhicules de service et en partie aussi les véhicules logistiques peuvent être remplacés par des véhicules dotés de modes de propulsion alternatifs tels que les piles à combustible, le moteur à combustion à hydrogène ou la propulsion électrique par batterie. Cependant, pour les véhicules militaires tactiques et lourds, ainsi que pour les avions et les hélicoptères, les possibilités sont très limitées. Pour les véhicules militaires légers, il existe l'option de remplacer le moteur à combustion par des alternatives. Toutefois, cela n'est pas possible sans faire de compromis en ce qui concerne la capacité à durer et la charge utile. L'utilisation de véhicules de démonstration équipés de motorisations alternatives doit donc être testée en détail sur le terrain. Outre les caractéristiques techniques, il ne faut pas non plus négliger le fait que l'infrastructure de ravitaillement ou de recharge doit être repensée et mise en place. L'utilisation de véhicules à propulsion alternative ne doit pas seulement fonctionner en situation normale, mais doit également être garantie en particulier dans les situations extraordinaires.

Les carburants liquides joueront encore longtemps un rôle important dans les véhicules militaires lourds et dans les Forces aériennes. Les hydrocarbures ont de loin la densité de puissance la plus élevée et ne peuvent donc pas être remplacés sans inconvénients majeurs en termes de poids et d'espace nécessaire. De plus, la logistique pour le transport des carburants liquides est connue, efficace et éprouvée. Les carburants durables, appelés Sustainable Aviation Fuels (SAF), sont toutefois déjà disponibles en petites quantités, en particulier sous l'impulsion de l'aviation civile. Il existe une offre limitée de biocarburants durables et la production de carburants synthétiques, produits par les technologies dites Power-to-X (PtX), va également connaître une très forte augmentation dans les années à venir. En outre, l'hydrogène est une source d'énergie importante, généralement produite par des procédés d'électrolyse. Le souhait de l'armée est de produire une partie des carburants durables en Suisse pour ses propres besoins.

Les immeubles du DDPS doivent à l'avenir être approvisionnés en électricité et en chaleur provenant entièrement de sources renouvelables, et si possible issues de leur propre production. Cela permet non seulement de réduire les émissions de CO2, mais aussi de soutenir l'objectif d'autarcie énergétique. Pour ce faire, la production d'électricité en propre doit être fortement augmentée. Outre l'accent mis actuellement sur l'énergie solaire, d'autres sources d'énergie sont également disponibles. La production d'énergie durable étant très variable selon les jours et la saison, il faut également s'attaquer au problème du stockage limité de l'énergie. Cela est essentiel afin que la défense puisse garantir son propre approvisionnement en énergie à tout moment. Le couplage sectoriel, c'est-à-dire le lien entre les secteurs énergétiques de l'électricité, du chauffage et du transport via un système de gestion de l'énergie, jouera un rôle important dans ce contexte.

L'énergie ne doit pas seulement être disponible sur les sites fixes, mais aussi pour les troupes en mission. Aujourd'hui, l'alimentation en électricité sur le terrain est assurée par défaut par des générateurs diesel. Pour les remplacer, il faut soit utiliser des générateurs fonctionnant avec des sources d'énergie durables comme l'hydrogène, soit assurer une fourniture d'énergie durable au moyen de solutions de stockage comme les accumulateurs. Il est important de les utiliser correctement, à la fois pour prolonger leur durée de vie et garantir la sécurité.

Thèmes de recherche 2025-2028

Concepts de mobilité et utilisation dans l'armée

- Études de technologie et de marché sur les concepts de propulsion alternatifs tels que les piles à combustible à hydrogène, la propulsion électrique par batterie, la propulsion hybride ou les moteurs à combustion fonctionnant de manière durable pour les véhicules militaires
- Développement de véhicules de démonstration militaires à propulsion électrique, à pile à combus-

tible ou à moteur à combustion fonctionnant de manière durable
- Tests approfondis des véhicules de démonstration militaires sur le terrain et en service
- Étude de la possibilité d'hybridation des véhicules et systèmes actuels de l'armée
- Clarifications concernant la sécurité des batteries et des réservoirs d'hydrogène en service, par exemple en cas de tirs
- Élaboration d'un modèle d'infrastructure pour le ravitaillement ou la recharge des véhicules militaires
- Études technologiques et études de marché concernant les petits avions à propulsion électrique ou à pile à combustible et évaluation du potentiel d'utilisation en tant qu'avions-écoles

Carburants durables

- Évaluation et comparaison des procédés de fabrication de carburants biogènes ou synthétiques
- Études de faisabilité et démonstration de mesures de réduction des coûts pour la production de carburants de synthèse
- Évaluation du potentiel et étude de faisabilité concernant la production de carburants synthétiques en Suisse
- Étude de la qualité et des propriétés des carburants durables produits par différents procédés tels que Fischer-Tropsch ou HEFA
- Étude de l'impact des carburants durables sur le fonctionnement et la durée de vie des moteurs des véhicules militaires
- Expérimentation de différentes applications de l'hydrogène dans un contexte militaire

Fourniture d'énergie durable pour les infrastructures

- Suivi des technologies de production d'électricité durable dans les domaines de l'énergie solaire, de l'énergie hydraulique, de l'énergie éolienne, de la géothermie, de la biomasse ainsi que de leur utilisation combinée
- Études de faisabilité et évaluation de méthodes appropriées pour la production locale d'énergie sur des sites sélectionnés de l'armée
- Observation des développements concernant le stockage de grandes quantités d'énergie grâce à des technologies telles que les batteries, les réservoirs d'air comprimé ou la transformation de l'électricité en vecteurs d'énergie tels comme l'hydrogène ou le méthane
- Démonstration de technologies de production et de stockage d'énergie dans l'environnement de l'armée
- Élaboration d'un concept pour l'exploitation en îlot de sites sélectionnés de l'armée et choix des technologies appropriées
- Mise en évidence des possibilités d'application du couplage sectoriel sur les sites de l'armée
- Étude et démonstration de concepts de courant de secours durables

Approvisionnement en énergie pour les troupes mobiles

- Recensement des besoins en électricité typiques des troupes et dans les camps militaires
- Évaluation de méthodes alternatives de production locale d'électricité sur le terrain
- Suivi et évaluation des technologies actuelles et disponibles à l'avenir pour les solutions d'approvisionnement en énergie portables pour le soldat
- Étude de l'utilisation de principes de production d'électricité fonctionnant avec de l'énergie primaire renouvelable ou des énergies secondaires durables, telles que l'hydrogène et le méthanol
- Mise en évidence des possibilités d'utilisation de l'hydrogène dans l'environnement mobile
- Étude de la sécurité des batteries, des systèmes à hydrogène et d'autres systèmes de stockage d'énergie

3.4.2 Simulation et analyse

Situation de départ et problématique

DLes possibilités de simulation et d'analyse ont considérablement progressé ces dernières années, et ce grâce à l'amélioration de la puissance de calcul et des capacités logicielles, d'une part, et aux développements continus des algorithmes, d'autre part. Les développements les plus remarquables ont été menés par des acteurs civils dans différents domaines tels que le calcul haute performance, l'intelligence artificielle (IA), les jumeaux numériques, les simulations multiphysiques et multidomaines et les simulations en temps réel.

Toutes ces améliorations technologiques ouvrent d'excellentes possibilités dans le domaine militaire,

en particulier lorsque l'armée est confrontée à des tâches d'une grande complexité, à des risques particuliers et à d'importants besoins en personnel et en matériel. Dans un tel contexte, il est souvent difficile de prendre des décisions fondées sur des aspects tels que les modalités d'engagement, le développement des forces armées ou l'optimisation des processus. La formation des soldats sur des systèmes leur permettant d'accomplir leurs missions constitue également un défi majeur. Certes, les expériences réalisées dans un environnement réel et les entraînements effectués avec des systèmes réels peuvent, dans certains cas, aider jusqu'à un certain point. Mais malheureusement, ces expériences et entraînements sont souvent trop coûteux, trop lents ou trop risqués pour être utilisés de manière extensive. Dans ce contexte, les simulations informatiques peuvent offrir une alternative intéressante en tant que reflet de la réalité. De plus, elles peuvent impliquer une réduction de la consommation de ressources et des émissions de CO2. Il y a cependant trois grands défis à relever. Le premier consiste à créer progressivement des plateformes de simulation universelles qui sont synergiques et compatibles ; celles-ci sont intégrées dans des systèmes déjà existants et elles peuvent interagir avec ces derniers, selon les besoins. Deuxièmement, il faut suivre le rythme des évolutions technologiques, qui sont très rapides dans ce domaine. En troisième lieu, les plateformes de simulation doivent être suffisamment flexibles pour permettre un éventuel transfert vers une nouvelle technologie plus performante.

Pour établir le lien avec la question initiale, il faut disposer d'outils permettant d'analyser des données issues de simulations. Les applications possibles peuvent être classées dans les catégories suivantes :

1. développement des forces armées,
2. appui à l'engagement,
3. formation.

Dans le domaine du développement des forces armées, des concepts sont développés pour permettre à l'armée de prendre en compte l'évolution des conditions-cadres. Pour ce faire, on suit notamment un processus appelé Concept Development and Experimentation (CD&E). Outre le travail de création de concepts proprement dit, des expériences sont donc également menées ici pour créer de nouvelles stratégies, contrôler des hypothèses et effectuer des vérifications. Les simulations peuvent apporter une contribution précieuse à cet égard.

Dans le cadre de l'appui à l'engagement, la priorité est donnée aux prises de décision à court terme. Les périodes de prévision s'étendent sur quelques semaines ou sur quelques heures, et il peut même s'agir d'applications en temps réel. Afin que la modélisation, la simulation et l'analyse soient disponibles dans les délais pour ces applications critiques en termes de temps, elles sont souvent regroupées dans des applications dédiées.

Le complexe d'applications Formation utilise quant à lui la simulation pour créer des scénarios tactiques virtuels dans lesquels des personnes à former peuvent être entraînées. L'objectif de tels simulateurs n'est pas toujours d'atteindre le plus grand réalisme possible. Au lieu de cela, l'accent est mis sur l'utilisation efficace de systèmes en réseau et sur la communication au sein des unités et entre elles. Pour cela, il faut une architecture de simulation qui permette une gestion centralisée des données dans un environnement utilisateur holistique décentralisé. Dans la simulation en temps réel, les représentations de cibles basées sur la réalité augmentée ainsi que les tirs virtuels remplaceront les simulateurs de tirs au laser classiques.

Dans toutes les catégories d'applications, les exigences en matière de modélisation, de simulation et d'analyse sont différentes. Dans tous les cas, un modèle dédié est nécessaire. Les modèles originaux (« out-of-the-box ») ne sont disponibles que dans des cas exceptionnels en raison de la forte spécialisation. En raison de la complexité des systèmes globaux, il est également nécessaire de développer ces modèles sur la base de l'état le plus récent de la recherche.

Thèmes de recherche 2025-2028

Simulation pour le développement des forces armées

- Étude d'algorithmes et de modèles pour le soutien dans le processus CD&E concernant le développement de l'armée
- Développement d'algorithmes d'IA pour l'optimisation au niveau tactique et opérationnel

Simulation pour l'appui à l'engagement

- Étude des approches de l'IA pour l'analyse et l'optimisation de la planification de l'engagement
- Développement d'outils pour l'aide à la décision basée sur les données

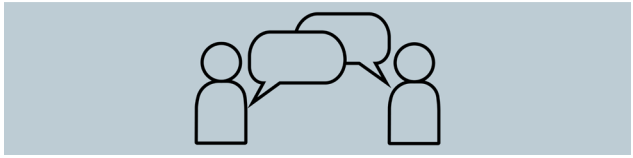
Simulation pour la formation et l'entraînement

- Étude des possibilités d'entraînement tactique personnalisé de soldats et de décideurs grâce à l'intelligence artificielle
- Suivi et vérification expérimentale des technologies, et ce aussi bien pour la représentation de la cible au moyen de la réalité augmentée (RA) en tir réel que pour son remplacement par le tir numérique

Thèmes transversaux de simulation et analyse

- Étude de procédures d'apprentissage automatique pour l'évaluation et l'interprétation automatisées de données de simulation
- Développement de modèles de jumeaux numériques pour représenter le paysage du système d'information de l'armée
- Étude de la faisabilité d'un environnement de simulation holistique avec une gestion centrale des données et des possibilités d'analyse en utilisant des capacités de science des données ainsi qu'avec une utilisation décentralisée de la simulation

3.4.3 Facteurs humains (human factors)



Situation de départ et problématique

Les facteurs humains jouent un rôle crucial dans la performance d'organisations telles que l'armée, qui doivent fonctionner de manière fiable dans toutes les situations. Comme les facteurs humains sont importants pour le succès de presque toutes les activités militaires, ils doivent être considérés comme un domaine transversal au sein de l'armée suisse. Les facteurs humains peuvent être considérés d'une part dans le contexte individuel, mais jouent également un rôle dans le contexte opérationnel et organisationnel.

Dans le contexte individuel, il s'agit de réduire les erreurs humaines et d'augmenter les performances des militaires. Les systèmes technologiques deviennent de plus en plus complexes et posent des exigences accrues à l'utilisateur. La collaboration entre les hommes et les machines doit également fonctionner afin de pouvoir profiter pleinement des possibilités technologiques. Si les systèmes ne peuvent pas être utilisés de manière intuitive et requièrent des connaissances spécialisées, les utilisateurs se sentent alors rapidement dépassés. Les systèmes et instruments technologiques doivent pouvoir être utilisés de manière à simplifier le processus de prise de décision et non à le rendre plus compliqué. Pour améliorer les performances humaines, il faut considérer à la fois les aspects psychologiques et physiques. Les technologies dites de « human enhancement » (amélioration humaine), comme la médecine personnalisée ou les biocapteurs, connaissent actuellement des développements rapides qui pourraient bientôt être appliqués dans l'environnement militaire. Une attention particulière devrait être accordée aux méthodes de mesure et d'évaluation des fonctions vitales dans des conditions de stress physique et psychologique. Cela permet, d'une part, d'améliorer les critères de sélection des militaires hautement spécialisés effectuant des tâches exigeantes et, d'autre part, de composer des plans d'entraînement personnalisés. Souvent, les exigences humaines ne sont identifiables que lorsque des missions ou des projets concrets sont en cours. Il s'agit alors de quantifier et de contrôler les effets des facteurs humains et de fournir ainsi une base pour des interventions basées sur des données. Pour ce faire, il existe en principe une multitude de méthodes et de procédés issus du domaine spécialisé des facteurs humains, qui peuvent être sélectionnés, adaptés et harmonisés entre eux pour une application dans le contexte militaire.

Les facteurs humains influencent les performances d'organisations entières. C'est pourquoi il est important de renforcer aussi bien la résilience de militaires individuels que celle de l'ensemble des forces armées. Une organisation résiliente doit à la fois être capable de développer une certaine robustesse face aux impondérables et de réagir et de s'adapter avec souplesse aux changements fondamentaux. Dans un monde de plus en plus complexe et ambigu, la résistance à la guerre cognitive va gagner en importance. Cette manière non conventionnelle et subversive de régler les conflits est de plus en plus utilisée et vise à influencer la perception humaine, la capacité de se forger une opinion et, en fin de compte, le comportement des individus et des groupes. Internet et les réseaux sociaux permettent une diffusion rapide des informations et une interaction rapide entre les participants, qu'il s'agisse de personnes ou d'agents conversationnels artificiels. Ainsi, dans le cadre de la guerre cognitive, la formation de "bulles" peut être contrôlée et la perception des gens peut être manipulée de manière ciblée par des informations tendancieuses ou fausses.

À long terme, cela peut influencer tout un système de valeurs, déstabiliser des organisations ou diviser des sociétés entières.

Thèmes de recherche 2025-2028

Human Enhancement (amélioration humaine)

- Suivi des tendances technologiques pour l'amélioration des performances humaines dans des domaines tels que la médecine personnalisée, les biocapteurs, la biotechnologie et l'interaction homme-machine
- Développement de méthodes pour améliorer les performances des soldats et des pilotes
- Élaboration de bases pour l'évaluation des aspects éthiques et juridiques des technologies d'amélioration humaine
- Compréhension du fonctionnement de la guerre cognitive et évaluation de son impact sur les individus, les troupes et la population
- Développement d'instruments pour aider les personnes dans les processus de décision

Quantification des facteurs humains

- Développement continu de méthodes d'évaluation de l'influence humaine sur l'efficacité des systèmes et des processus
- Évaluation de l'acceptation de l'intelligence artificielle et estimation de son influence sur les décisions humaines
- Étude des interactions entre les hommes et les machines et mise en évidence du potentiel de développement continu
- Élaboration de méthodes pour la constitution d'équipes efficaces

Résilience

- Exploration des possibilités de renforcement de la résilience individuelle des militaires
- Évaluation de la capacité de la défense à réagir et à s'adapter aux changements, à anticiper les menaces et les opportunités futures et à identifier ses propres vulnérabilités
- Développement d'un modèle de résilience des forces armées sur la base des besoins de l'Armée suisse

4 Financement

4.1 Financement 2021-2024

En Suisse, le financement public de la recherche en matière de politique de sécurité ayant une pertinence pour la défense est assuré exclusivement par le DDPS. D'autres instruments de la Confédération, comme le Fonds national suisse ou Innosuisse, excluent la recherche purement liée à la défense. Toutefois, dans de nombreux cas, les technologies à double usage peuvent être utilisées aussi bien à des fins civiles qu'à des fins militaires. Il n'est donc pas possible d'établir une séparation nette entre la recherche civile et la recherche liée à la défense. Outre la recherche financée par les pouvoirs publics, l'industrie de l'armement implantée en Suisse investit également dans la recherche liée à la défense. Les investissements précis de l'industrie privée ne sont pas ventilés selon la recherche et le développement et ne donnent donc pas une image cohérente par rapport aux dépenses dans la recherche de l'administration fédérale.

Les dépenses de recherche d'armasuisse se composent de prestations propres (intramuros) et du financement de mandats confiés à des partenaires de recherche externes (extramuros)(Illustration 8). Les prestations propres comprennent la gestion de la recherche, la conduite de programmes de recherche et la réalisation interne de projets sous la forme d'un calcul des coûts complets. L'attribution de contrats de recherche à des partenaires universitaires et industriels se fait sur la base de mandats et de projets. Depuis 2019, les dépenses liées à la recherche ont fortement augmenté. Cela est principalement lié à la création du Cyber-Defence Campus et à l'augmentation des effectifs et du budget de recherche qui en découlent.

4.2 Financement 2025-2028

Le fait de lier l'orientation stratégique de la recherche d'armasuisse à l'engagement financier correspondant est considéré comme étant digne de protection, car l'accomplissement des tâches d'une partie de l'administration fédérale ou d'une partie de l'armée peut être entravé s'il est connu. C'est pourquoi ces informations doivent être classées CONFIDENTIELLES conformément à l'article 6, let. e de l'ordonnance concernant la protection des informations de la Confédération (OPrI, RS 510.411) et au catalogue de classification établi par la Conférence des secrétaires généraux. Les indicateurs financiers sont fournis dans un appendice classifié du plan de recherche à long terme. Le présent document sans appendice n'est soumis à aucune classification.

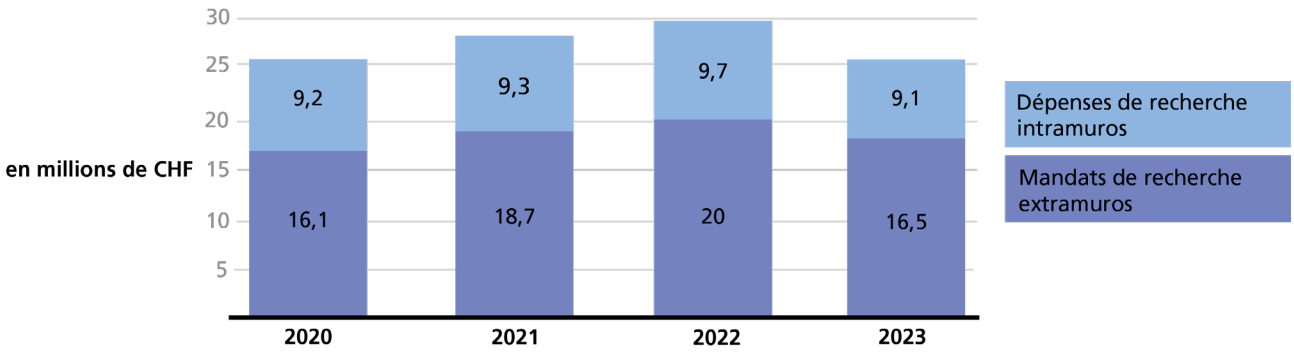


Illustration 8: Dépenses de recherche d'armasuisse pour la période 2019 - 2023.

5 Acteurs et interfaces

5.1 Description des principaux acteurs

La recherche d'armasuisse a pour but d'assurer les compétences qui permettent de réaliser pour les forces de sécurité de la Suisse, en particulier pour l'armée, le Service de renseignement et l'Office fédéral de la cybersécurité, des expertises indépendantes à la pointe de la science et de la technique. En outre, les compétences issues de la recherche constituent une base importante pour la promotion et la mise en œuvre d'innovations à caractère technologique. En accord avec les parties prenantes de l'environnement des instruments de la politique de sécurité, armasuisse pilote la recherche, et ce du niveau stratégique jusqu'à la mise en œuvre dans des projets. armasuisse oriente le réseau de compétences en fonction des besoins et veille au transfert des connaissances acquises à partir des projets de recherche vers les processus de stratégie, de planification, d'innovation et d'acquisition du DDPS.
Un tel réseau doit être mis en place de manière stratégique et durable. Les partenariats sont conçus pour le moyen ou le long terme et sont basés non seulement sur les compétences initiales de l'institution de recherche mais aussi sur des intérêts communs en termes de contenu, notamment pour les technologies ayant un potentiel d'application pour les forces de sécurité. Le réseau national de compétences peut être divisé en quatre catégories de partenaires différentes (Illustration 9).

- **Les hautes écoles et les instituts scientifiques à but non lucratif : outre les deux écoles polytechniques fédérales de Zurich et de Lausanne, les Universités de Zurich et de Berne ainsi que plusieurs hautes écoles spécialisées sont des partenaires de recherche importants. Afin de renforcer la collaboration, armasuisse S+T a conclu des accords de partenariat stratégiques, et ce dans le domaine de la robotique avec l'EPF de Zurich et dans le domaine de l'exploration radar avec l'Université de Zurich. En outre, un conseil technologique a été créé au niveau du Département. Il est composé de représentants de haut rang du DDPS et de l'EPF de Zurich. Il existe avec l'EPFL des partenariats stratégiques dans le cadre du Cyber-Defence Campus et du Space Campus. Les hautes écoles et les instituts constituent l'épine dorsale scientifique de la recherche axée sur les aspects techniques au sein du DDPS.**

- **Les start-up sont intéressantes en tant que partenaires de recherche, car elles essaient très souvent de mettre sur le marché de nouveaux produits basés sur des développements technologiques de pointe réalisés par les hautes écoles. Dans de nombreux cas, le milieu des start-up se distingue par son indépendance d'esprit et sa volonté d'essayer de nouvelles choses, ce qui contribue largement au développement dynamique de systèmes économiques. Selon la phase de développement des start-up, elles apportent des contributions importantes en matière de recherche appliquée en réalisant des démonstrateurs, ou alors elles sont des partenaires importants dans la réalisation de projets d'innovation à caractère technologique. La collaboration avec les start-up est généralement limitée dans le temps, soit parce qu'une grande partie d'entre elles sont rachetées par des entreprises établies, soit parce que la percée espérée de l'idée commerciale n'a pas lieu. armasuisse observe de près le milieu des start-up en Suisse, car elles constituent un indicateur important des développements technologiques.**

- **En Suisse, il n'est pas rare que les petites et moyennes entreprises (PME) se distinguent par une grande spécialisation et des produits de pointe dans le domaine de la haute technologie. Celles-ci ne peuvent maintenir leur position que si elles évoluent en permanence. Pour armasuisse, ces entreprises sont particulièrement intéressantes lorsque leur pipeline de produits présente un fort potentiel de double usage. Il s'agit de déterminer l'impact de ces technologies sur les applications des forces de sécurité et les adaptations nécessaires pour répondre aux exigences de leur environnement.**

- **La collaboration avec des entreprises d'armement classiques est également intéressante, en particulier avec celles qui disposent de leurs propres départements de recherche et de développement en Suisse. Certes, elles sont axées sur leur gamme de produits et ne couvrent donc pas, loin s'en faut, toutes les technologies pertinentes. Néanmoins, ce sont des partenaires importants qui peuvent fournir, grâce à leurs connaissances approfondies, de précieuses prestations d'intégration de technologies modernes sur des plateformes existantes à des fins de démonstration. En outre, ils**

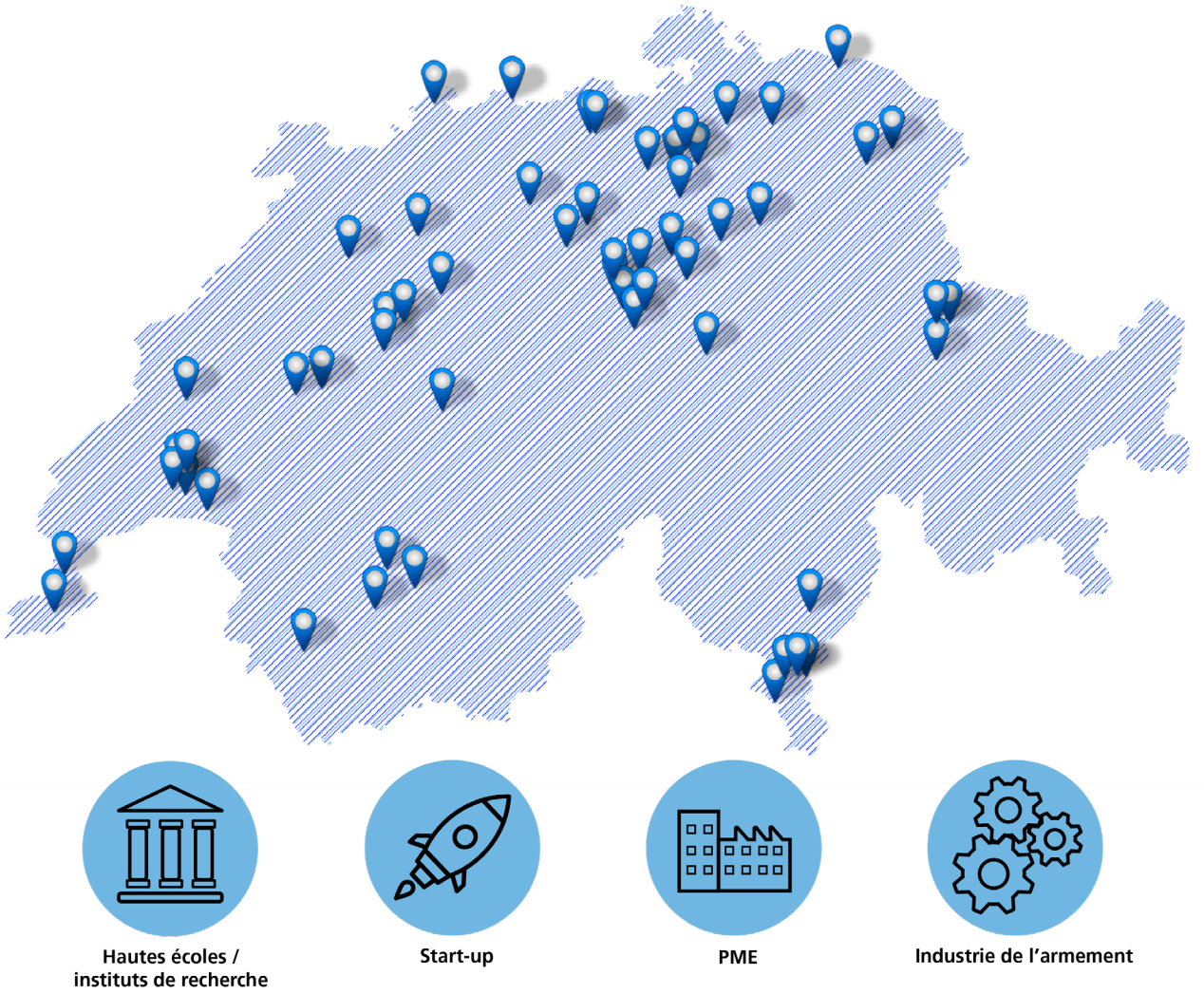


Illustration 9: Catégories de partenaires du réseau de compétences d'armasuisse.

peuvent fournir des prestations d'ingénierie et de soutien importantes dans le cadre de projets d'innovation.

Il convient de faire évoluer en permanence pour les forces de sécurité suisses le vaste réseau de compétences, et ce en fonction des besoins et des progrès technologiques réalisés dans les technologies clés. Le développement des connaissances à l'aide de réseaux s'effectue dans le cadre de projets et en tant que mandat visant à clarifier des aspects concrets de la recherche (recherche contractuelle). Dans ce cadre, le partenaire de recherche est évalué à l'avance selon le principe de l'add-on. Cela signifie que l'attribution du mandat s'oriente en premier lieu sur les compétences déjà existantes du partenaire de recherche et que, dans la mesure du possible, seuls les aspects qui sont spécifiques aux forces de sécurité sont définis comme objet de recherche. En se concentrant sur un degré de maturité technologique compris entre 3 et 5, on évite en outre d'investir dans la recherche fondamentale, qui est en principe alimentée par d'autres sources comme le FNS.

Mais il existe aussi des technologies destinées aux forces de sécurité pour lesquelles il n'existe en Suisse des partenaires de recherche appropriés que dans des domaines sélectionnés. De telles lacunes peuvent en partie être comblées grâce à des coopérations avec des partenaires de recherche étrangers. Mais dans ce cas, les projets de recherche peuvent en partie également être réalisés directement au sein d'armasuisse.

5.2 Interfaces avec d'autres offices fédéraux

La coordination des interfaces avec d'autres offices fédéraux et organisations liées à la Confédération dans le domaine de la recherche est assurée par le Comité interdépartemental de coordination de la recherche de l'administration. Des groupes de travail et des ateliers permettent d'identifier les intérêts communs des différents offices fédéraux afin d'exploiter les synergies lors de l'élaboration des différents plans directeurs de recherche et d'éviter les doublons. En outre, cette plateforme offre également la possibilité d'échanger avec le FNS et Innosuisse, les deux principales organisations nationales d'encouragement de la recherche et de l'innovation. Ainsi, armasuisse a également la possibilité, au niveau spécialisé, de prendre position par rapport aux propositions du FNS dans le cadre des programmes nationaux de recherche (PNR) et des pôles de recherche nationaux (PRN), d'une part, et de commenter les programmes phares d'Innosuisse, d'autre part. La recherche de l'administration d'armasuisse peut ainsi opérer une transition en douceur par rapport aux instruments nationaux d'encouragement de la recherche et de l'innovation.
La coordination avec d'autres offices fédéraux a permis d'identifier les domaines thématiques de coopération suivants :

- Office fédéral de la protection de la population (OFPP) : recherche dans les domaines des biotoxines et de la détection des armes biologiques, mesure et cartographie de la radioactivité à l'aide de drones, analyse des tendances et protection des infrastructures critiques.
- Office fédéral de l'énergie (OFEN) et Office fédéral de l'aviation civile (OFAC) : participation au programme d'encouragement « SWiss Energy research for the Energy Transition » (SWEET) pour la production de kérosène synthétique dans le cadre du plan d'action « Energie et climat DDPS ».
- Office fédéral de la cybersécurité : soutien technique par le biais d'analyses de tendances et d'activités de recherche dans le cadre de la mise en œuvre de la cyberstratégie nationale (CSN).
- Division Sécurité internationale (DSI) au Secrétariat d'État du Département fédéral des affaires étrangères (DFAE) : conseils techniques dans les domaines de l'intelligence artificielle et de la robotique dans le cadre de négociations multilatérales.

En outre, il existe dans le cadre de la recherche de l'administration fédérale, pour le domaine politique « Politique de sécurité et de paix », un groupe de travail composé de représentants de l'OFPP, de la DSI et de l'Office fédéral de l'armement (armasuisse). Sur la base des directives en matière de politique de sécurité et de paix, ce groupe de travail élabore les lignes directrices des plans directeurs de recherche et coordonne leur mise en œuvre opérationnelle dans des domaines thématiques et des projets prioritaires.

5.3 Coopération internationale

Le rapport complémentaire au rapport sur la politique de sécurité 2021 indique notamment que la coopération internationale de la Suisse doit être renforcée dans le domaine de la politique de sécurité et de sa mise en œuvre. Même si l'OTAN poursuit le format de collaboration actuel, le « Partenariat pour la paix » (PPP), elle s'est quand même mise en quête d'une collaboration sur mesure avec des États partenaires, ce qui convient à la Suisse. L'OTAN et la Suisse ont ainsi défini les objectifs stratégiques de leur coopération dans un programme de partenariat personnalisé (Individually Tailored Partnership Programme, ITPP) qui prévoit notamment d'approfondir la coopération technique et scientifique par l'établissement d'un dialogue stratégique et la mise en œuvre pratique sous la forme de projets communs de recherche, d'innovation et de développement. En ce qui concerne la recherche, cela signifie un renforcement de l'engagement au sein de l'Organisation pour la science et la technologie (Science and Technology Organisation, STO) de l'OTAN. Pour cela, la Suisse doit être représentée dans des groupes de pilotage (panels) supplémentaires. En ce qui concerne l'innovation, l'Accélérateur d'innovation de défense pour l'Atlantique Nord (Defence Innovation Accelerator for the North Atlantic, DIANA) constitue une plateforme de collaboration idéale. L'offre de la STO s'étend des cours de formation dans certains domaines technico-scientifiques à la réalisation d'études et de projets de recherche communs, en passant par des réunions d'experts sur des thèmes choisis. L'échange avec des experts internationaux et les activités de recherche communes apportent une très forte valeur ajoutée et des enseignements qui, autrement, ne pourraient guère être exploitées à un coût raisonnable. Les expériences concernant la participation aux activités de la STO et du PPP de l'OTAN sont toutes positives.

La signature d'un accord administratif avec l'Agence européenne de défense (AED) en 2012 permet à la Suisse de participer aux activités de recherche de l'AED. Celles-ci sont organisées en domaines technologiques basés sur les capacités, appelés CapTechs. L'objectif de ces CapTechs est de coordonner et d'encourager la collaboration européenne en matière de recherche, et notamment l'industrie, dans le domaine des technologies de défense. La Suisse est aujourd'hui représentée dans cinq CapTechs. Contrairement aux programmes-cadres de recherche de la Commission européenne, le financement des projets CapTech est réparti entre les pays participants, ce qui entraîne un effort de coordination considérable et aussi une certaine inefficacité. L'engagement du Hub for European Defence Innovation (HEDI) ouvre à la Suisse de nouvelles possibilités dans la mise en œuvre de ses projets d'innovation et constitue ainsi une suite logique des activités menées dans le cadre des CapTechs.

Enfin, la collaboration internationale a également lieu dans le cadre de traités internationaux, d'accords de coopération bilatéraux ou trilatéraux et d'accords techniques qui en découlent. On vise ici une coopération avec des instituts d'État ou financés par l'État à l'étranger, qui peuvent très souvent faire état de compétences spécifiques concernant des technologies pour les forces de sécurité, qui ne sont pas disponibles en Suisse. Outre la coopération bilatérale avec les pays proches, il convient de mentionner qu'un document d'entente a été signé dans le cadre d'un accord trilatéral entre l'Allemagne, l'Autriche et la Suisse (DACH) en 2023, qui vise à simplifier la coopération en matière de recherche et de développement militaires entre les trois pays. En outre, il existe également depuis 2019 un accord Research, Development, Test and Evaluation (RDT&E) (recherche, développement, test et évaluation) qui permet des coopérations avec des laboratoires de recherche des forces armées américaines.

6 Organisation et assurance qualité

6.1 Organisation interne

Au sein d'armasuisse, le domaine de compétences Sciences et technologies est responsable de la direction et de la réalisation de la recherche. Ces tâches sont réalisées dans le cadre du groupe de prestations NMG attribué « Gestion des technologies et expertises ». La gestion des technologies est une activité transversale qui va de la détection précoce et de l'évaluation des technologies à l'établissement de feuilles de route technologiques pour d'éventuelles acquisitions, mais avec un accent sur l'interface entre les programmes de recherche et les différents vecteurs d'innovation au sein du DDPS. L'objectif n'est pas seulement de réduire les risques technologiques et financiers, mais aussi de participer à la planification militaire globale. Pour accomplir cette mission, armasuisse S+T mène des activités de recherche appliquée ciblées afin de développer des compétences technologiques indispensables à l'accomplissement à moyen terme des missions du DDPS. La CODA ainsi que la convention sur la collaboration entre le domaine départemental Défense et armasuisse Sciences et technologies du 16 novembre 2017 constituent les bases de l'harmonisation des activités de recherche avec les besoins de la planification militaire globale.

Le domaine spécialisé « Gestion de la recherche et recherche opérationnelle » est responsable de l'élaboration du plan de recherche à long terme et de la planification annuelle de la mise en œuvre. Le PRLT est validé par le directeur général de l'armement une fois que la consultation a eu lieu au sein du département. Le responsable du domaine de compétences S+T autorise la planification annuelle de la mise en œuvre. Les axes de recherche prévus avec les domaines thématiques prioritaires du présent PRLT sont traités par des programmes de recherche axés sur les capacités nécessaires et futures de l'Armée suisse. Les responsables de programme désignés définissent la priorité du contenu des programmes de recherche par des analyses systématiques des besoins auprès des parties prenantes concernées et assurent leur mise en œuvre. La surveillance de la recherche, composée de représentants de l'état-major de l'armée et d'armasuisse S+T, veille à l'orientation stratégique correcte du portefeuille de programmes et à son financement. Elle se focalise sur l'adéquation, l'efficacité et la rentabilité de la recherche d'armasuisse.

Les programmes de recherche regroupent généralement plusieurs champs de compétences à traiter à moyen et à long terme, dans lesquels différents projets sont traités. Afin de fournir à l'armée et aux forces de sécurité le transfert de connaissances de la recherche au profit de l'activité d'expertise, la direction du projet est assurée au sein des domaines spécialisés d'armasuisse S+T. La mise en œuvre de la recherche se fait sous la forme d'une structure matricielle, ce qui permet d'actualiser les compétences des experts internes en fonction de l'état actuel de la technique et de la science. Les projets de recherche sont en partie traités en interne, mais dans de nombreux cas avec des partenaires issus des hautes écoles et de l'économie, dans le cadre de ce que l'on appelle la recherche contractuelle. L'attribution de mandats de recherche se base sur la loi fédérale sur les marchés publics (LMP, RS 172.056.1). Les contrats de recherche sont attribués en grande partie sur la base des Conditions générales de la Confédération relatives aux contrats de recherche, élaborées par le Département fédéral des finances (DFF) et la Conférence des achats de la Confédération (CA). Toute dérogation à ces règles est consignée par écrit dans le contrat de recherche. Cela concerne notamment les droits de publication et l'exploitation de la propriété intellectuelle créée dans le cadre du mandat de recherche. La gestion de projet suit les normes internationales de gestion de projet afin de garantir la qualité. La qualité scientifique des travaux de recherche est garantie à la fois par une sélection rigoureuse de l'institution de recherche et par une évaluation des travaux et des découvertes scientifiques.

6.2 Assurance qualité

En 2014, le Comité interdépartemental de coordination de la recherche de l'administration a édicté des directives relatives à l'assurance qualité dans la recherche de l'administration fédérale, qui comprennent trois volets : la gestion de la recherche, les rapports et le contrôle de l'efficacité. La mise en œuvre du concept d'assurance qualité relève de la responsabilité des services fédéraux et peut être adaptée de manière flexible aux circonstances.

Chez armasuisse, les mesures d'assurance qualité suivantes ont été mises en œuvre durant la période 2021-2024 :

- La disponibilité en temps utile de compétences pour la réalisation d'expertises, qui est un objectif principal de la recherche, a été relevée dans le cadre des objectifs du budget avec plan intégré des tâches et des finances (B/PITF) du groupe de prestations « Gestion technologique et expertises » et évaluée en termes de degré de réalisation. Le cas échéant, des mesures ont été prises en conséquence.
- La CODA et le concept de développement des forces orienté capacités (WE DFOC) ont défini l'harmonisation des activités de recherche avec les besoins de la planification militaire globale.
- Les processus de la recherche avec la réglementation correspondante des compétences, qui sont consignés dans le système de gestion intégré (SGI) d'armasuisse, ont été soumis à une révision régulière et audités par un organisme indépendant dans le cadre de la recertification (ISO 9001).
- Afin de garantir une orientation adéquate des programmes de recherche, les domaines de compétences correspondants ont fait l'objet d'un contrôle annuel et ont été coordonnés avec les parties prenantes lors d'un atelier. L'examen du portefeuille de programmes de recherche et des domaines thématiques prioritaires a été effectué chaque année par la surveillance de la recherche.
- Afin de garantir la mise en place ciblée de réseaux d'experts, des partenaires de recherche potentiels ont été systématiquement évalués. L'application « Suivi de la technologie et du marché » est développée afin d'accroître l'efficacité des évaluations systématiques. La nouvelle version devrait être opérationnelle d'ici 2025.
- La qualité scientifique de la recherche a été assurée en collaborant de préférence avec des partenaires de recherche qui jouissent d'une excellente réputation sur le plan national et international et qui publient régulièrement dans des revues et à l'occasion de conférences spécialisées reconnues.
- Les travaux de recherche ont régulièrement fait l'objet de discussions avec des experts scientifiques internes et externes, de sorte que la qualité des résultats de la recherche a pu être vérifiée par un deuxième avis et par l'avis de tiers.
- Les compétences en matière de gestion de projet dans l'environnement de la recherche ont été renforcées, permettant aux collaborateurs de bénéficier de mesures de formation continue internes ou externes, comme l'obtention d'un certificat de l'International Project Management Association (IPMA) ou le suivi de la formation Certificate of Advanced Studies in Research Management.

Les mesures suivantes sont prévues pour la période 2025-2028 :

- Les mesures d'assurance qualité de la période 2021-2024 sont maintenues ou poursuivies. Cela inclut notamment la révision des processus internes, l'enregistrement et l'évaluation de l'efficacité des activités de recherche, la garantie de l'orientation des thèmes de recherche en fonction des besoins et la garantie de la qualité scientifique des résultats et des enseignements tirés.
- La formation continue des collaborateurs scientifiques est activement encouragée, tant au niveau technique qu'au niveau de la gestion.
- Afin d'augmenter l'attractivité d'armasuisse S+T en tant qu'employeur pour de jeunes scientifiques talentueux, des activités communes telles que des bourses de recherche (fellowships), des concours, des universités d'été, des stages ou des conférences sont encouragées en coopération avec des établissements de formation universitaires.
- La qualité des travaux scientifiques en cours réalisés par des partenaires externes est évaluée à l'aide d'instruments appropriés. En dehors des audits externes, une enquête réalisée au moyen d'un système d'enquête interne est en principe également envisageable.
- La qualité du transfert des connaissances et des enseignements tirés de la recherche, qui vise à encourager les innovations dans l'environnement des forces de sécurité, est renforcée. Cela nécessite une collaboration plus étroite entre armasuisse S+T et les différents responsables de l'innovation au sein du DDPS, notamment par l'application de méthodes créatives modernes, d'une gestion de projet agile ainsi que d'approches basées sur des groupes de réflexion.

6.3 Diffusion des connaissances

Les différents programmes de recherche d'armasuisse, avec leurs nombreux projets de recherche et leurs nombreuses coopérations, produisent une grande quantité de connaissances. Chez armasuisse S+T, les projets de recherche sont encadrés par des collaborateurs de l'organisation hiérarchique. Cela permet de garantir que les compétences scientifiques sont mises en place là où elles sont nécessaires au sein de l'organisation pour réaliser des expertises. Des mesures internes spéciales pour le transfert des enseignements tirés

au sein d'armasuisse S+T ne sont donc plus nécessaires. Cependant, il est important d'avoir une stratégie permettant d'obtenir un transfert des connaissances optimal vers les différents partenaires impliqués. Pour atteindre cet objectif, les résultats sont rendus accessibles autant que possible, et ce sous différentes formes telles que des rapports annuels, des événements divers tels que des ateliers, des présentations de projets et des symposiums, la participation à des conférences ou la publication dans des revues scientifiques. Il est également important de mentionner que les connaissances issues de la recherche ne sont pas seulement mises à disposition pour le développement des forces orienté capacités, mais aussi pour des projets d'innovation potentiels, leur évaluation, leur mise en œuvre et, enfin, pour le transfert des résultats dans la troupe. De plus, cela doit permettre d'assurer le transfert des enseignements tirés de la recherche vers l'armée par le biais de la planification de l'armée. La réalisation d'une plateforme de gestion des connaissances pour la diffusion des enseignements tirés de la recherche est à l'étude.

Les informations sur les projets, telles que les données complètes sur l'état d'avancement des projets et leurs résultats, y compris les rapports de recherche, sont stockées et mises à jour électroniquement sur ARAMIS (Administration Research Actions Management Information System). ARAMIS est le système d'information électronique concernant les projets de recherche et de développement de la Confédération. Pour un public plus large, chaque programme de recherche dispose de son propre site Internet, sur lequel sont publiées des informations générales telles que des fiches d'information, des domaines de compétences et différents rapports.

Annexe 1 : Répertoire des abréviations

Abréviation	Signification
3D	En trois dimensions
5G	5e génération (téléphonie mobile)
ACAMIL	Académie militaire
AED	Agence européenne de défense
ar	armasuisse
ARAMIS	Administration Research Actions Management Information System
B/PITF	Budget avec plan intégré des tâches et des finances
BLA	Base logistique de l'armée
BTIS	Base technologique et industrielle importante pour la sécurité
C2	Command and Control
CA	Conférence des achats de la Confédération
CapTech	Capability Technology (Group of EVA)
CCD CoE	Cooperative Cyber Defence Centre of Excellence (centre d'excellence pour la cyberdéfense en coopération)
CD&E	Concept Development and Experimentation
Cdmt	Commandement
CENAL	Centrale nationale d'alarme
CO2	Dioxyde de carbone
CODA	Directives concernant la collaboration entre les domaines départementaux Dé-fense et armasuisse
COTS	Commercial Off-the-Shelf
COVID-19	Maladie à coronavirus
CRCA	Réseau de capteurs, de renseignement, de conduite et d'action
CSDR	Centre Suisse des Drones et de la Robotique
CSN	Cyberstratégie nationale
CSS	Center for Security Studies (de l'EPF de Zurich)
Cst.	Constitution fédérale
CYBEEM	Cyberespace et espace électromagnétique
D	Domaine départemental Défense
DACH	Allemagne, Autriche, Suisse
DDoS	Distributed Denial of Service
DDPS	Département de la défense, de la protection de la population et des sports
DEVA	Développement de l'armée
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DIANA	Defence Innovation Accelerator for the North Atlantic (Accélérateur d'innovation de défense pour l'Atlantique Nord)
DM BDA	Doctrine militaire base doctrinale de l'armée
DPDH	Division Paix et droits de l'homme
DSI	Division Sécurité Internationale
EM A	État-major de l'armée
EPFL	École polytechnique fédérale de Lausanne
EPFZ	École polytechnique fédérale de Zurich
ESA	Agence spatiale européenne
FED	Fonds européen de la défense
fedpol	Office fédéral de la police (Federal Police)
FNS	Fonds national suisse

Abréviation	Signification
FOSKE	Développement des forces armées axé sur les capacités
FRI	Formation, recherche et innovation
GEOINT	Geospatial Intelligence
GNSS	Global Navigation Satellite Systems
GTP	Generative Pre-trained Transformers
HALE	High Altitude Long Endurance
HAP	High Altitude Platform
HEDI	Hub for European Defence Innovation
HEFA	Hydroprocessed Esters and Fatty Acids
HPM	High Power Microwaves
HUMINT	Human Intelligence
IA	Intelligence artificielle
IdO	Internet des objets
IED	Improvised Explosive Device
IEM	Impulsion électromagnétique
IMINT	Image Intelligence
IPMA	International Project Management Association
ISO	International Standardisation Organisation
ITPP	Individually Tailored Partnership
LAAM	Loi sur l'armée
LERI	Loi sur l'encouragement de la recherche et de l'innovation
LMP	Loi fédérale sur les marchés publics
LRens	Loi fédérale sur le renseignement
LSI	Loi fédérale sur la sécurité de l'information au sein de la Confédération
MALE	Medium Altitude Long Endurance
MASINT	Measurement and Signature Intelligence
MOTS	Military off-the-Shelf
NASA	National Aeronautics and Space Administration
NBC	Nucléaire, biologique, chimique
NMG	Nouveau modèle de gestion de l'administration fédérale
OFAC	Office fédéral de l'aviation civile
OFEN	Office fédéral de l'énergie
OFPP	Office fédéral de la protection de la population
OFS	Office fédéral de la statistique
O-LERI	Ordonnance relative à la loi fédérale sur l'encouragement de la recherche et de l'innovation
OMat	Ordonnance du DDPS sur le matériel
OMP	Ordonnance sur les marchés publics
ONU	Organisation des Nations unies
OODA	Observe-Orient-Decide-Act
OPrI	Ordonnance concernant la protection des informations
ORens	Ordonnance sur le renseignement
Org	Ordonnance sur l'organisation
OSCE	Organisation pour la sécurité et la coopération en Europe
OSRA	Ordonnance concernant le Service de renseignement de l'armée
OTAN	Organisation du Traité de l'Atlantique Nord
OTAN/PPP STO	OTAN/PPP Science and Technology Organisation
PESTEL	Political, Economic, Social, Technological, Legal, Environment

Abréviation	Signification
PITF	Planification intégrée des tâches et des finances
PME	Petites et moyennes entreprises
PNR	Programmes nationaux de recherche
PPP	Partenariat pour la paix
PRLT	Plan de recherche à long terme
PRN	Pôles de recherche nationaux
PtX	Power-to-X
RA	Réalité augmentée
RADINT	Radar Intelligence
RDT&E	Research, Development, Test and Evaluation
RO	Règlement d'organisation
ROSO	Renseignement d'origine sources ouvertes
RS	Recueil systématique du droit fédéral
RSO	Radar à synthèse d'ouverture
RUAG	RüstungsUnternehmen-AktienGesellschaft (société anonyme d'entreprise d'armement)
S+T	Domaine de compétences Sciences et technologies d'armasuisse
SAF	Sustainable Aviation Fuels
SDR	Software Defined Radio
SF Données D	Stratégie de fonctionnement Données Défense
SGI	Système de gestion intégré
SIGINT	Signal Intelligence
SOCMINT	Social Media Intelligence
SRC	Service de renseignement de la Confédération
STO	Organisation pour la science et la technologie (de l'OTAN)
SWEET	SWiss Energy research for the Energy Transition
TIC	Technologies de l'information et de la communication
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle
UE	Union européenne
UGV	Unmanned Ground Vehicle
USA	États-Unis d'Amérique
USB	Universal Serial Bus
VISINT	Visual Intelligence

Annexe 2 : Bases légales et documents stratégiques

Niveau Confédération

- Constitution fédérale (Cst.) RS 101, art. 2 But, art. 57-60 Sécurité, défense nationale, art 64. Recherche, 1er janvier 2024
- Rapport du Conseil fédéral, La politique de sécurité de la Suisse, 24 novembre 2021
- Rapport du Conseil fédéral, Rapport complémentaire au Rapport sur la politique de sécurité 2021 concernant les conséquences de la guerre en Ukraine, 7 septembre 2022
- Cyberstratégie nationale (CSN), 13 avril 2023
- Loi fédérale sur l'encouragement de la recherche et de l'innovation (LERI), RS 420.1, en particulier art. 16, art. 42, art. 45, 1er juillet 2023
- Ordonnance relative à la loi fédérale sur l'encouragement de la recherche et de l'innovation (O-LERI), en particulier les art. 24 à 25, RS 420.11, 1er septembre 2023
- Ordonnance relative au système d'information ARAMIS sur les projets de recherche et d'innovation de la Confédération (Ordonnance ARAMIS), RS 420.171, 1er janvier 2014.
- Loi fédérale sur la sécurité de l'information au sein de la Confédération (LSI), RS 128, 1er janvier 2024
- Ordonnance concernant la protection des informations de la Confédération (OPrI), RS 510.411, 1er septembre 2023
- Loi fédérale sur les marchés publics (LMP), RS 172.056.1, 1er janvier 2024
- Ordonnance sur les marchés publics (OMP), RS 172.056.11, 1er septembre 2023
- Assurance qualité dans la recherche de l'administration fédérale - Directives, 1re révision du 26 mars 2014
- Principes pour l'élaboration des concepts 2025-2028 concernant les activités de recherche de l'administration fédérale dans les 11 domaines politiques, octobre 2022
- Politique spatiale 2023, 19 avril 2023
- Loi fédérale sur l'utilisation de l'espace exoatmosphérique (en cours d'élaboration)

Niveau DDPS

- Loi fédérale sur l'armée et l'administration militaire (loi sur l'armée, LAAM), RS 510.10, 1er janvier 2024
- Ordonnance du DDPS sur l'acquisition, l'utilisation et la mise hors service du matériel (OMat), RS 514.20, 18 août 2020
- Directives relatives à la collaboration entre les domaines départementaux Défense et armasuisse (CODA), 28 mars 2018
- Ordonnance sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (Org-DDPS), RS 172.214.1, 1er janvier 2024
- Règlement d'organisation du DDPS (RO-DDPS), 1er janvier 2024
- Stratégie cyber DDPS 2021-2024, mars 2021
- Ordonnance sur la cyberdéfense militaire (OCMil), RS 510.921, 1er janvier 2024
- Loi fédérale sur le renseignement (LRens), RS 121, 1er janvier 2024
- Ordonnance sur le service de renseignement (Ordonnance sur le renseignement, ORens), RS 121.1, 1er janvier 2024
- Principes du Conseil fédéral en matière de politique d'armement du DDPS, 24 octobre 2018
- Stratégie d'armement du DDPS, 1er janvier 2020
- Stratégie de département du DDPS, vision, champs d'action et initiatives stratégiques, 15 septembre 2022
- Plan d'action Énergie et climat DDPS, juin 2021

Niveau domaine départemental Défense

- Renforcer la capacité de défense - Objectifs et stratégie 2023, Centre des médias numériques de l'armée MNA, 81.298d
- Rapport de base sur la défense aérienne du futur, La sécurité de l'espace aérien pour protéger la Suisse et sa population, mai 2017
- Rapport de base sur l'avenir des forces terrestres, développement des capacités des forces terrestres, mai 2019
- Rapport de base Conception générale Cyber, conception du développement des capacités de l'Armée suisse dans le cyberespace et l'espace électromagnétique jusqu'au milieu des années 2030, février 2022
- Rapport de base sur la conception globale de l'espace exoatmosphérique (en cours d'élaboration)
- Doctrine militaire 2017 - Bases doctrinale de l'armée (doctr mil 17 BDA), 7 juillet 2019
- Base doctrinale du cyberespace et de l'espace électromagnétique (CYBEEM), projet, état au 31 mars 2023
- Ordonnance concernant le Service de renseignement de l'armée (OSRA), RS 510.291, 1er septembre 2023
- Planification des investissements de l'armée de 2023 à 2035, 7 septembre 2022
- Message sur l'armée (annuel)

Niveau domaine départemental armasuisse

- Règlement d'organisation de l'Office fédéral de l'armement, 15 août 2017
- Système de gestion armasuisse (SGI ar) : Gestion de la technologie et de la recherche (processus Id 2.20.25 et doc. Id 40031)
- PITF : Plan intégré des tâches et des finances armasuisse 2025-2027, volume 2A, groupe de prestations « Gestion technologique et expertises » (p. 347-351), 24 août 2023
- Plan de recherche à long terme 2021-2024 (Sciences et technologies, armasuisse), 30 novembre 2020