Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS
Armée suisse

CONCEPTION GÉNÉRALE CYBER

Conception du développement des capacités de l'Armée suisse dans le cyberespace et l'espace électromagnétique (CYBEEM) d'ici au milieu des années 2030.

Contenu

Contenu

Contenu

Illustrations

Tableaux

Résumé

La Conception générale cyber met en évidence d'une part les défis du cyberespace et de l'espace électromagnétique (CYBEEM) et d'autre part ceux des technologies de l'information et de la communication (TIC) ; elle décrit ensuite les capacités que l'Armée suisse devra développer d'ici 2035 environ pour être à même de faire face aux défis à venir.

Cette évolution se place dans le cadre du développement de l'armée en tant que système intégral (administration, domaines spécialisés, armes et services auxiliaires), puisqu'elle en influence des pans entiers.

La guerre actuelle en Ukraine confirme que le CYBEEM est devenu une dimension centrale de l'exercice du pouvoir et ceci tant pour la préparation que la conduite d'un conflit, aussi bien dans le domaine civil que militaire. Il sert entre autres à l'exercice de la puissance ainsi qu'à la préparation et à la conduite des conflits. Ces dernières années, des États et des acteurs non étatiques ont effectué des campagnes de désinformation et de propagande, entravé les télécommunications civiles et commis des attaques par le biais de maliciels. De plus en plus de cyberattaques ont en outre pris pour cibles des infrastructures énergétiques et des autorités. Il est nettement plus difficile de remonter la piste des attaques dans le CYBEEM que celles menées de manière classique et il est moins aisé de retrouver leurs auteurs ou l'État par lequel elles ont été commanditées. Il est par conséquent souvent impossible de prononcer des sanctions contre leurs auteurs, ce qui favorise le passage à l'acte.

Le cyberespace de l'armée englobe tous les systèmes informatiques exploités et utilisés par l'armée (systèmes TIC). Toutes les données et informations ainsi que l'ensemble des usagers des systèmes TIC existants font également partie du cyberespace. L'espace électromagnétique sert en particulier à la transmission (électromagnétique) d'informations par radio ainsi qu'à la localisation et à l'identification d'objets dans l'espace. Le CYBEEM met en réseau les différents espaces d'opération physiques (sol, air, espace maritime, espace exo-atmosphérique). Il est dès lors d'une importance capitale pour chaque opération militaire de pouvoir utiliser à notre profit les capacités propres au CYBEEM et de les garder sous notre contrôle. La conduite opérative doit par conséquent pouvoir planifier, diriger et piloter les engagements de l'armée de manière intégrale, à travers tous les espaces d'opération et avec les moyens adéquats, afin de pouvoir en tout temps atteindre l'effet visé. Pour que l'armée puisse accomplir sa mission, il est essentiel qu'elle protège ses propres systèmes TIC et ses propres données et informations face aux menaces variées du CYBEEM, dans toutes les situations et pour toutes les composantes de l'armée.

La Conception générale cyber place le principe de la supériorité en matière de savoir et de décision comme élément-clé du succès à l'engagement. Celui qui agit le premier peut placer la partie adverse dans le rôle de celui qui doit réagir et ainsi prendre la main sur le déroulement des événements. C'est ainsi qu'à l'engagement, c'est vraisemblablement la partie qui disposera dans les meilleurs délais d'une image complète de la situation qui sera en mesure de prendre les bonnes décisions pour mener au succès. Pour atteindre son objectif, il faut pouvoir prendre et gagner l'initiative en engageant ses moyens, par nature limités, à temps et avec précision.

L'armée se trouve dans un champ de tensions multidimensionnel. Elle doit en effet non seulement remplir ses missions actuelles, mais aussi, pour rester dans la course, anticiper à temps les menaces et les défis futurs ainsi que les évolutions toujours plus rapides dans le CYBEEM. Cela implique des processus d'adaptation rapide. Étant donné que les opérations de l'armée vont en règle générale impliquer toutes les possibilités du CYBEEM, elle doit acquérir des capacités globales concernant tous les espaces d'opération, des capacités dont elle ne dispose pas encore aujourd'hui.

La présente conception générale met en exergue la question de savoir quelles sont les capacités dont l'armée devra disposer dans le CYBEEM et dans les TIC à compter de 2030, afin de pouvoir s'acquitter de sa mission à long terme dans toutes les situations. Elle clarifie également la question de savoir dans quelle mesure l'armée peut ou doit aussi appuyer des partenaires (p. ex. OFPP, RNS, autres services fédéraux et autorités, partenaires économiques et de la société) dans la maîtrise de ces défis. Les premiers chapitres portent sur les tendances lourdes concernant l'environnement et l'évolution constatées dans contexte tant national qu'international et décrit les bases doctrinales pour l'armée. Celles-ci sont regroupées en six capacités fondamentales, à savoir :

Trois options ont été élaborées sur cette base, qui prennent en considération les besoins de l'armée entière. Elles tiennent par ailleurs compte des évolutions et nouveautés futures issues des autres espaces d'opération et intègrent les capacités opérationnelles susmentionnées, à chaque fois sous différentes formes. Toutes ces options pourront être mises en œuvre d'ici 2035 environ sans incidence sur les effectifs, par des transferts au sein du Groupement Défense.

L'option 1 réunit les capacités cyber et électromagnétiques à l'échelon de l'armée. S'agissant du développement, l'accent est presque entièrement placé sur l'autoprotection CYBEEM et sur les capacités dans le cyberespace. Il n'est pas prévu de développer ces capacités jusqu'à l'échelon tactique inférieur (bataillon et compagnie), ni d'équiper des formations de combat avec les moyens requis. Il manque de ce fait une réponse adéquate à un possible conflit hybride dans un terrain aussi bâti que celui que l'on retrouve habituellement en Suisse.

L'option 2 donne les moyens à la majorité des formations des forces terrestres de mener de manière autonome des actions dans leur secteur dans le CYBEEM. De petites équipes spécialisées comprenant une dizaine de militaires sont constituées dans les compagnies de combat. Elles sont équipées de systèmes leur permettant de mener dans le CYBEEM des attaques d'ampleur réduite en suivant des procédés élémentaires. Un tel développement des capacités en largeur et en profondeur aurait cependant des inconvénients significatifs: non seulement les coûts seraient importants, mais les exigences techniques seraient élevées, car des systèmes largement automatisés seraient nécessaires qui ne sont pour l'heure pas encore disponibles dans le domaine cyber. On peut en outre se demander si l'armée serait à même de recruter autant de militaires de milice et de carrière disposant des connaissances et prédispositions appropriées.

L'option 3 a pour but de rendre l'armée capable de se protéger à l'avenir entièrement contre les attaques CYBEEM. Cette protection s'étend tant aux systèmes permanents qu'à ceux exploités de manière temporaire (p. ex. systèmes d'armes comprenant une importante composante TIC). Comparée aux autres options, celle-ci prévoit une bien plus grande autoprotection contre les menaces dans l'espace électromagnétique. L'autoprotection doit être assurée au niveau central, de sorte que les capacités requises, de très haute qualité, doivent être rassemblées, comme aujourd'hui, dans un bataillon spécialisé à l'échelon de l'armée. Il doit toutefois être possible de protéger les infrastructures-clés de manière ponctuelle et décentralisée. Des moyens du bataillon cyber peuvent être attribués ou subordonnés à d'autres formations de l'armée (ou si nécessaire à des partenaires civils) en fonction des besoins. En se concentrant sur l'autoprotection, l'armée met une importante exigence de la SNPC en œuvre, à savoir celle qui demande que tous les acteurs soient responsables de leur propre protection et doivent dès lors être en mesure de se protéger de manière aussi autonome que possible des risques et des menaces du cyberespace.

Placées côte à côte, les trois options s'illustrent de la manière suivante :

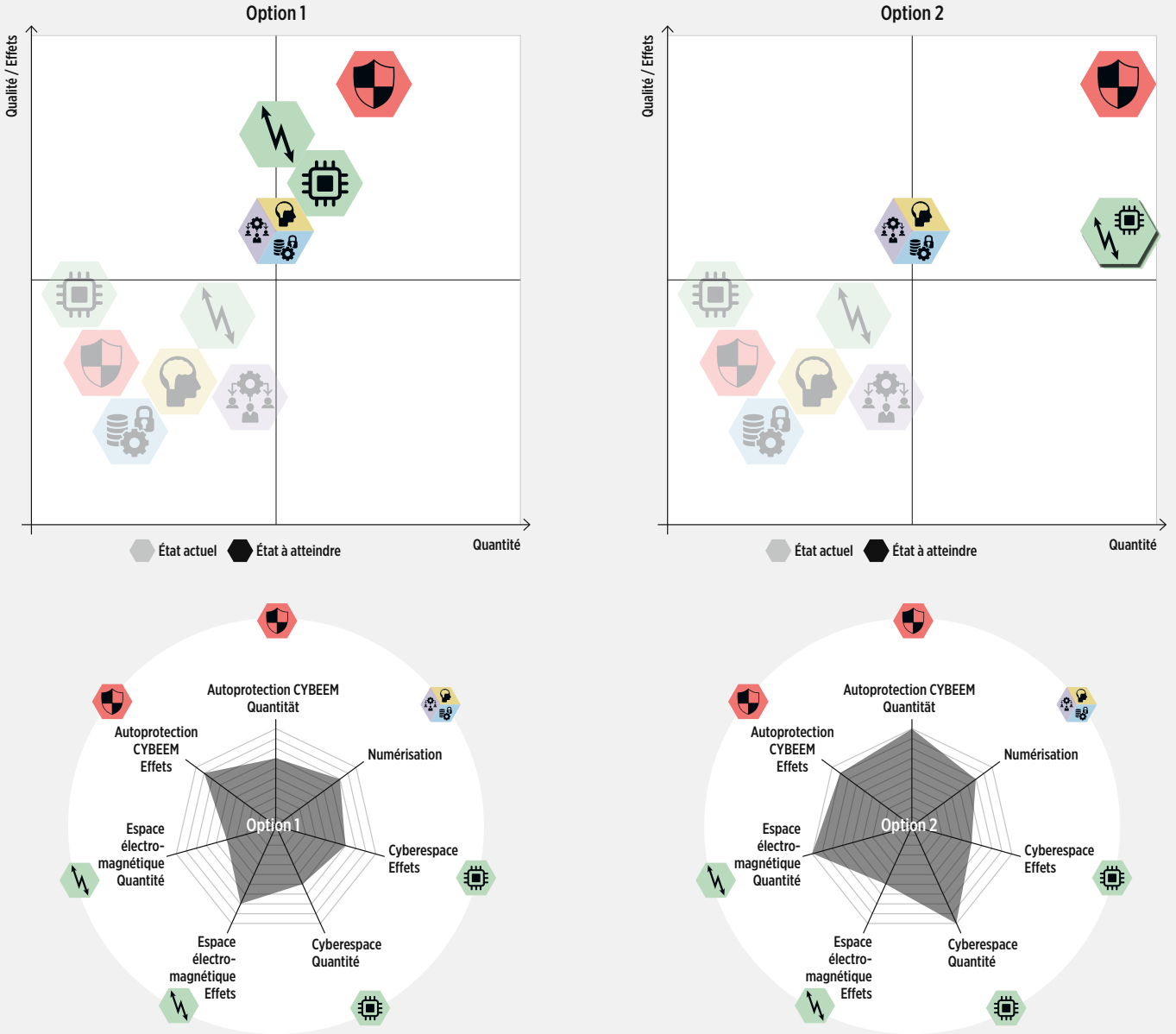
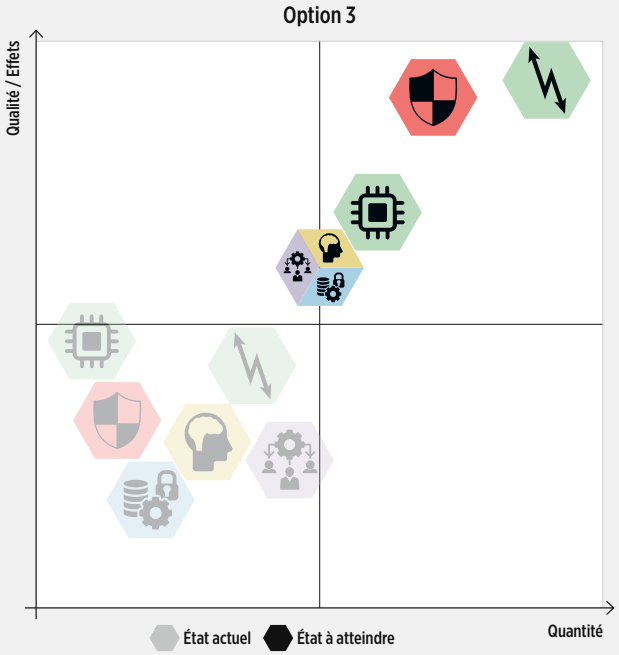
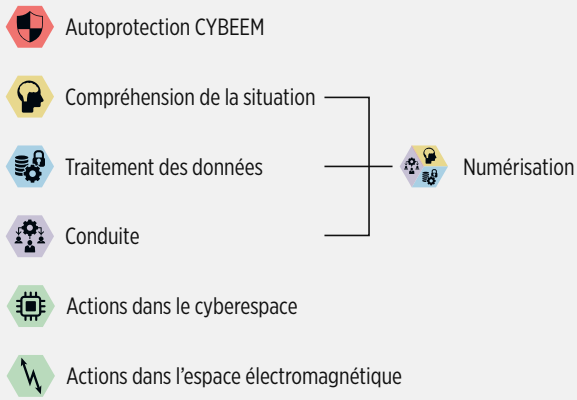
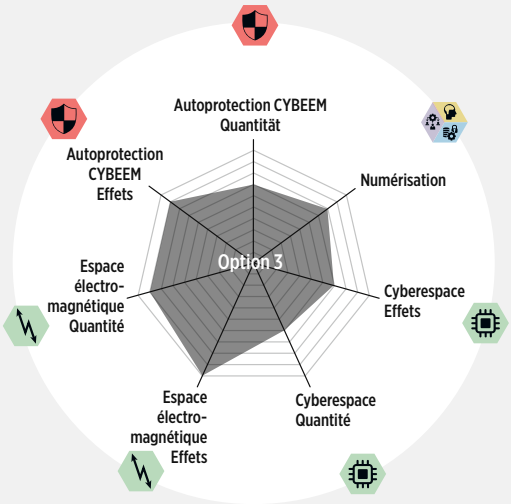


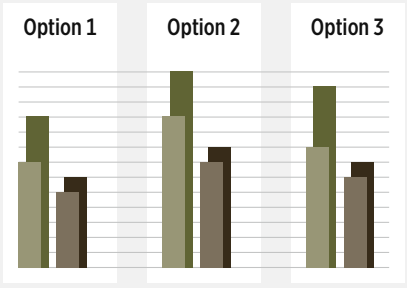
Illustration 1: représentation graphique des trois options

S'appuyant sur l'analyse effectuée, le groupe d'experts du DDPS propose de choisir l'option 3, car elle offre une utilité plus élevée sur le plan militaire, en ce sens qu'elle contribue grandement à l'exécution de la mission de l'armée. S'agissant par ailleurs de la situation du marché du travail en Suisse, le besoin estimé en spécialistes qualifiés est jugé réaliste. L'option 3 crée en outre de bonnes conditions pour pouvoir répondre aux défis futurs dans le CYBEEM. Globalement, elle offre un profil de capacités et de prestations équilibré et orienté sur l'avenir, lequel permettra à l'armée de s'acquitter de sa mission à partir de 2030.









Option	Coûts d'investissement Mia CHF	Troupe Militaires
1	1,4 – 2,0	5000 – 6000
2	2,0 – 2,6	7000 – 8000
3	1,6 – 2,4	6000 – 7000

Coûts d'exploitation/an : environ 15% des coûts d'investissement

La mise en œuvre de l'option 3 doit se dérouler en trois étapes. Les objectifs généraux de chacune d'entre elles sont décrits ci-après :

L'étape 1 vise en priorité à poursuivre le renforcement centralisé de l'autoprotection CYBEEM existante ainsi qu'à maintenir et en partie à étendre les capacités permettant de mener des actions dans le cyberespace et l'espace électromagnétique. La capacité fondamentale en matière d'application de la science des données est par ailleurs renforcée. La science des données consiste en l'analyse d'importants lots de données, qui sont examinés dans le but de répondre à des questions stratégiques ou opérationnelles.

L'étape 2 vise à consolider la résilience des infrastructures-clés utilisées dans le cadre de l'autoprotection CYBEEM. La capacité servant à assurer la propre protection CYBEEM décentralisée et la forensique dans le secteur d'engagement est consolidée. Après la mise en œuvre de cette étape, une infrastructure informatique locale autonome (aussi appelée nœud local) devra être disponible pour la troupe, tout en tenant compte des besoins inhérents à la capacité de commandement de l'armée. Les capacités permettant de mener des actions dans le CYBEEM sont par ailleurs maintenues et en partie renforcées.

L'étape 3 vise à renforcer les capacités des bataillons et des compagnies à mener des actions autonomes dans l'espace électromagnétique jusqu'à l'échelon de la technique de combat. La capacité à se protéger contre des menaces émanant de l'espace électromagnétique est renforcée jusqu'à ce même échelon de conduite. À compter de 2032, les systèmes majeurs des forces terrestres devront en outre être renouvelés. Cette opportunité permettra d'intégrer directement sur ces nouvelles plateformes les systèmes actifs et d'autoprotection dans le domaine électromagnétique ou, tout au moins, de les harmoniser et ainsi de profiter des synergies en résultant. Dans le cyberespace, les capacités en matière d'exploration et d'intervention seront renforcées et adaptées aux nouvelles technologies.

L'illustration montre l'horizon temporel approximatif des étapes de mise en œuvre. Étant donné que certaines mesures sont mises en place sur le long terme et qu'il en résulte des interdépendances, il n'est pas possible de les distinguer clairement les unes des autres. Le tableau décrit donc quelles sont les mesures prioritaires pour chacune de ces étapes.

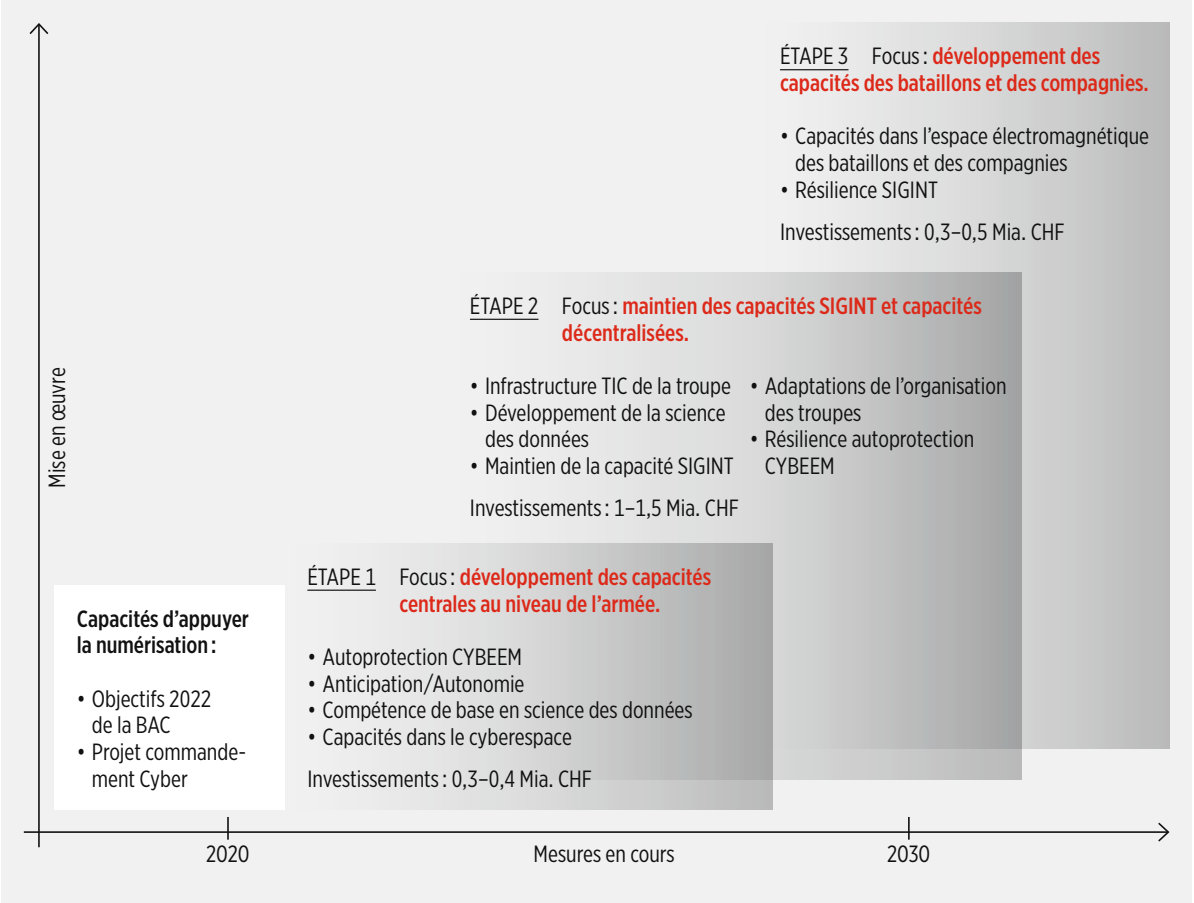


Illustration 2 : étapes de la mise en œuvre de l'option 3

1

Introduction

Les conflits actuels impliquent fortement le champ électromagnétique et le cyberespace. Au quotidien, l'Armée suisse et la société dans son ensemble sont déjà régulièrement confrontées aux cyberattaques. La numérisation croissante augmente notre vulnérabilité dans ce domaine. Le développement de l'armée exige donc de prendre en compte les défis du CYBEEM.

1 Introduction

On a assisté ces dernières années dans le cyberespace et l'espace électromagnétique (CYBEEM) à des changements conséquents et rapides. Ces évolutions, impliquant de manière réciproque l'un et l'autre de ces espaces, les ont rapprochés. Le résultat de cette convergence est qu'il est aujourd'hui quasiment impossible de faire la distinction entre la partie d'une action qui implique le cyberespace de celle dans l'espace électromagnétique. Dans le CYBEEM, les frontières géographiques comme celles qui existent en particulier au sol et dans l'espace aérien ne revêtent presque plus aucune importance. C'est la raison pour laquelle ces deux espaces d'opération sont habituellement regroupés dans un seul, le CYBEEM.

CYBEEM

Le CYBEEM désigne le cyberespace et l'espace électromagnétique, le champ TIC dans son intégralité ainsi que la logistique des données et de l'information [1].

Cyberespace de l'armée

Le cyberespace de l'armée englobe toutes les données et informations ainsi que les systèmes TIC exploités ou utilisés par l'armée, indépendamment de la zone des effets à laquelle ils sont physiquement affectés.

Espace électromagnétique

L'espace électromagnétique sert à la transmission technique d'informations (transmission par signal s'appuyant sur un réseau radio), à la localisation d'objets dans l'espace (radar, localisation radio) et à la conduite de la guerre électronique (GE), à l'aide d'ondes électromagnétiques de différentes fréquences.

L'interdépendance étroite des espaces d'opération au sein du CYBEEM est une réalité. Les modifications qui interviennent à l'intérieur de ce milieu sont souvent immédiates et influencent la plupart du temps ces deux espaces simultanément. Bien que virtuels, les effets des actions au sein du CYBEEM impactent toujours plus fortement par leurs conséquences les espaces physiques tels que l'espace terrestre, aérien, maritime ou exo-atmosphérique. Le CYBEEM gagne ainsi toujours plus en importance.

Cette évolution place la société, l'État et l'économie devant de nouveaux défis. Les interdépendances mutuelles engendrent un degré de complexité élevé. Le risque de perturbations augmente alors que les systèmes physiques et virtuels deviennent de plus en plus vulnérables. D'où une exigence accrue en termes d'autoprotection.

Un conflit moderne sans actions dans le CYBEEM n'est envisageable ni aujourd'hui ni demain. Dans ce contexte, l'Armée suisse doit en permanence être capable d'acquérir des renseignements, de se protéger, d'aider (subsidiairement) et de combattre de manière autonome, dans toutes les situations et de manière concertée au travers de tous les espaces d'opération. Il s'agit dès lors pour l'Armée suisse d'intégrer le CYBEEM comme moyen à part entière d'action dans la planification et l'exécution de ses engagements, de le protéger de manière autonome et de contribuer, où cela est nécessaire, à la protection dans ce domaine des partenaires essentiels à son action.

Cette réalité est particulièrement visible dans la guerre actuelle en Ukraine, qui est menée avec des moyens tant civils que militaires. Des institutions étatiques, des in-

1 La logistique des données et de l'information englobe le traitement, l'enregistrement et la distribution d'informations et de données au sein de l'Armée suisse.

frastructures critiques, les forces de sécurité et la société civile sont simultanément visées. Il s'agit d'un conflit hybride, tel que représenté dans le Rapport sur la politique de sécurité 2021 ainsi que le « Rapport sur l'avenir des forces terrestres ». Afin d'informer la société, et pour la conduite des opérations militaires, tous les moyens disponibles de communication civile et militaire sont employés. Garantir la sécurité du réseau du gouvernement et de l'armée devient une tâche décisive pour permettre la défense d'une nation. La protection contre des attaques cybernétiques est ainsi essentielle pour l'armée comme pour la société ; celle-ci constitue la première ligne de défense d'une nation.

La guerre en Ukraine confirme également que la clé pour la conduite avec succès d'opérations militaires réside dans la mise en réseau – à travers le CYBEEM – des senseurs avec les effecteurs. Plus les renseignements collectés par les éclaireurs, les drones et les autres sources d'information sont évalués et compilés rapidement dans une image intégrale de la situation, plus les cibles adverses peuvent être combattues de manière précise et rapide. Un grand impact peut être atteint avec des moyens proportionnellement réduits. A cette fin, l'acquisition de compétences pour assurer l'autoprotection du CYBEEM, la capacité d'exploiter le potentiel de la numérisation pour la conduite d'actions militaires et la liberté de manœuvre au sein du CYBEEM sont absolument nécessaires.

1.1 Raison d'être

L'armée a pour mission de protéger et de défendre la Suisse et sa population, d'apporter son appui aux autorités civiles, de sauvegarder la souveraineté sur l'espace aérien et de contribuer à maintenir la paix. Afin qu'elle puisse s'acquitter de l'ensemble de ces missions, elle doit pouvoir garantir la cohérence de ses actions à travers tous les espaces d'opération (cf. Illustration 3 : espaces d'opération).

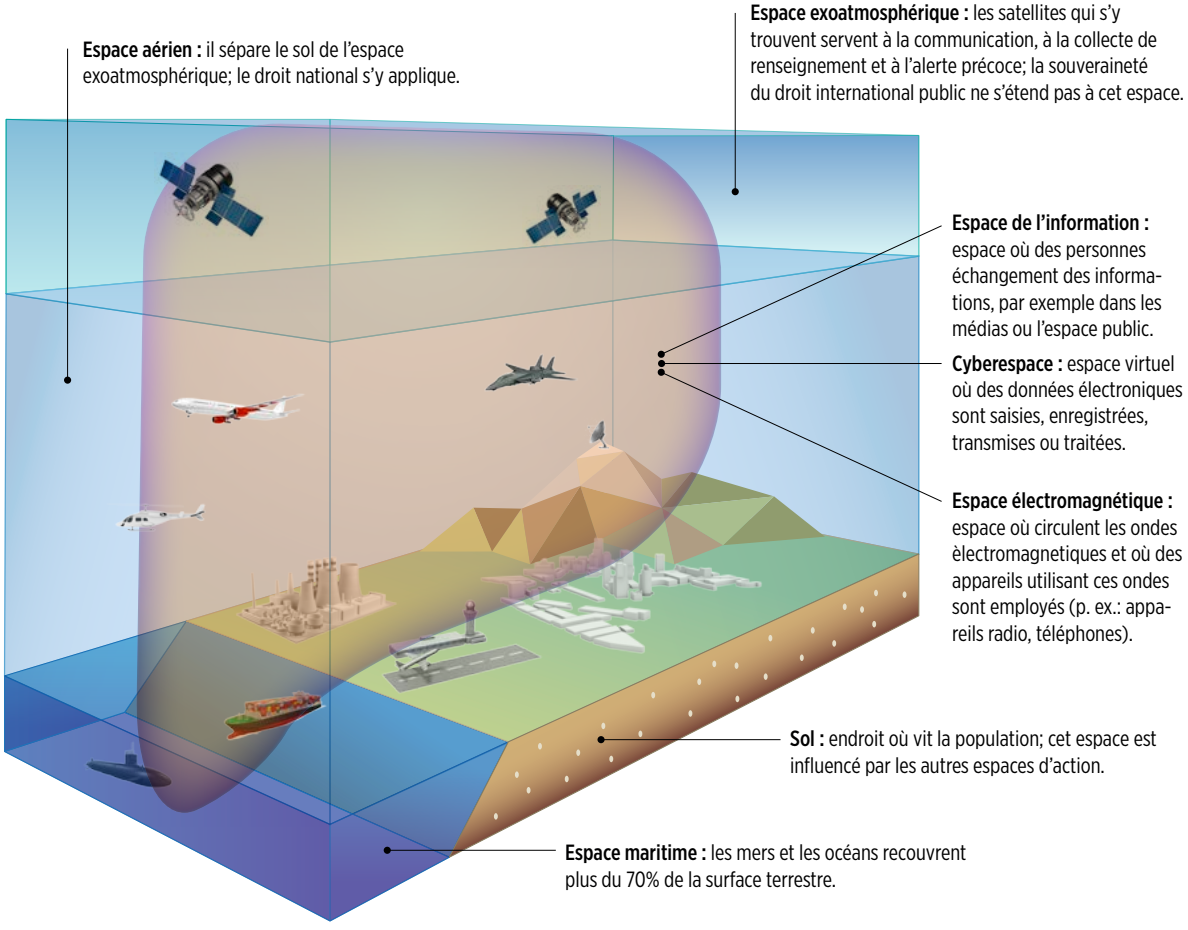


Illustration 3 : espaces d'opération

Comme décrit dans l'illustration 4, le CYBEEM constitue la colonne vertébrale qui intègre l'espace d'information et les espaces d'opération physiques que sont le sol, l'espace aérien, l'espace maritime et l'espace exo-atmosphérique. Il permet les échanges de données et d'informations entre capteurs, moyens d'action et commandement, également à travers les différents espaces d'opération. Les engagements de plus en plus complexes de l'armée ne peuvent être planifiés et conduits sans l'utilisation du CYBEEM.

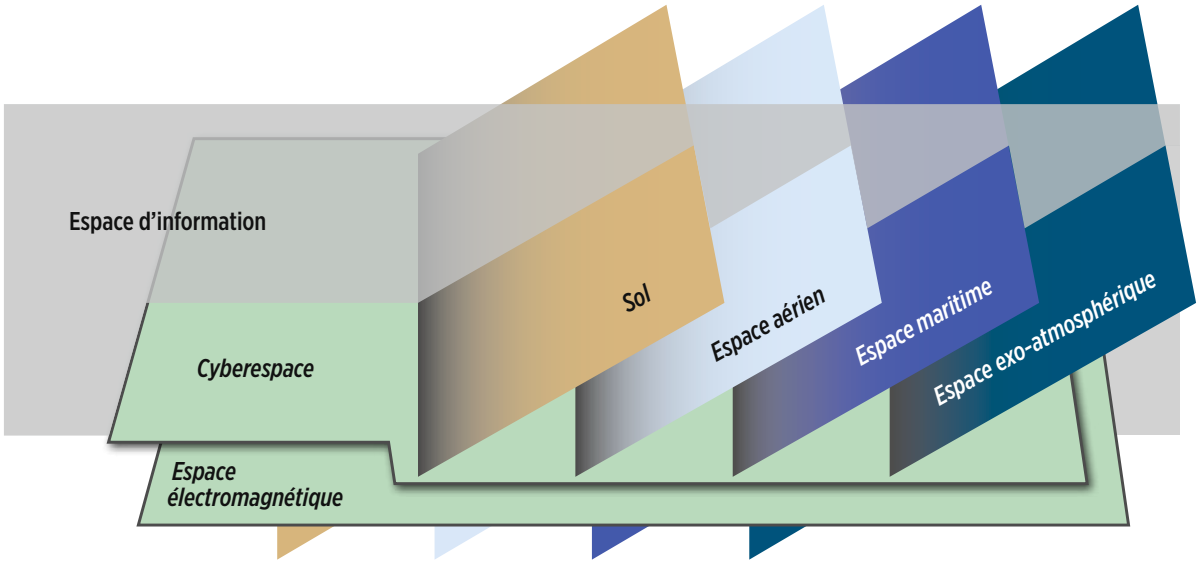


Illustration 4 : le CYBEEM – colonne vertébrale des autres espaces d'opération

1.2 But

La présente conception générale est destinée à définir les mesures nécessaires au développement des capacités dans le domaine du CYBEEM et des TIC. Elle permet de donner une image complète de ce domaine et formule les orientations majeures en matière de planification à l'horizon des deux prochaines décennies.

La conception reprend les constations faites dans les deux rapports précédents qui concernaient le développement à moyen et à long terme de l'armée : Avenir de la défense aérienne (2017) et Avenir des forces terrestres (2019), rapports qu'elle approfondit et concrétise sous l'angle du CYBEEM et des TIC. Elle se réfère également au Rapport sur la politique de sécurité 2021, à la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 (2018) et à la Stratégie cyber du DDPS (2021).

Il s'agit de présenter la thématique du CYBEEM et son importance pour l'orientation future de l'armée et pour la collaboration avec des partenaires dans un contexte plus large. Une attention particulière sera accordée aux aspects relevant du droit international ainsi qu'aux bases et conditions-cadres existantes.

La question centrale qui se pose est de savoir quelles sont les capacités dont l'armée devra disposer à l'avenir dans le CYBEEM afin de pouvoir remplir sa mission sur le long terme. Il s'agira par ailleurs de répondre à la question de savoir dans quelle mesure des partenaires doivent et peuvent être soutenus.

Afin de pouvoir répondre à ces questions, les thèmes ci-après doivent être mis en lumière :

a) La situation nationale et internationale et son évolution future ont un impact majeur sur le type de capacités CYBEEM que l'armée doit développer et sur la manière dont elle veut traiter les données et les informations. Jouent un rôle également l'évolution technologique, les questions liées à la numérisation, mais aussi les conditions-cadres inhérentes au secteur de la formation et à l'économie. Enfin, les concepts de l'armée doivent s'inscrire dans le cadre plus global de la Confédération, qui est par exemple décrit dans la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) ou dans la Stratégie Suisse numérique.

b) Différents acteurs mènent régulièrement des actions contre des objectifs en Suisse, également contre l'armée. Plusieurs cyberattaques contre des systèmes informatiques de l'armée ont ainsi pu être prouvées. L'exploration radio et l'exploration du réseau câblé sont également une réalité. Partout sur la planète, des actions sont menées pour influer sur les opinions à travers une diffusion ciblée d'informations. Les capacités de l'armée doivent dès lors aussi s'adapter à la menace concrète et quotidienne émanant du CYBEEM.

c) Les exigences envers le renouvellement à venir du système de surveillance de l'espace aérien et de conduite des opérations aériennes (C2Air), des nouveaux avions de combat et du système de défense sol-air montrent à quel point l'interconnexion des systèmes revêt une importance centrale. Afin que l'armée puisse engager ses moyens efficacement, les actions doivent être coordonnées de manière précise dans le temps. Le prérequis pour ce faire est une mise en réseau, tout à la fois numérisée et flexible, de capteurs, de moyens d'action et des organes de conduite. La mise en œuvre de ce dessein pose de grands défis afin d'instaurer une architecture TIC uniforme et oblige l'armée et l'administration militaire à standardiser leurs applications.

1.3 Situation initiale sur le plan du droit international

La Suisse est liée aux règles du droit international, en particulier aux garanties relevant des droits fondamentaux et humains ancrés dans la Constitution et le droit international public, que ce soit dans le monde virtuel ou analogique. Du point de vue du droit international, l'armée et les services de renseignement sont par principe soumis aux mêmes règles que d'autres organes étatiques. Leurs actions doivent dès lors respecter les directives correspondantes en matière de droit international.

Il s'agit de faire la distinction, d'une part, entre les règles générales du droit international, qui s'appliquent notamment en temps de paix, et celles inhérentes au droit humanitaire international[2], d'autre part, lesquelles s'appliquent exclusivement lors de conflits armés et qui sont également désignées comme droit international des conflits armés au sein de l'armée. Le droit international public vaut pour toutes les contre-mesures de l'armée et du service de renseignement en réaction à un cyberincident international, lorsque celui-ci touche à des systèmes d'information de l'armée ou à des infrastructures critiques de la Suisse, au-dessous du seuil d'une attaque armée[3]. Les principes ressortissants au droit international public de la souveraineté étatique[4], de l'interdiction d'intervention[5] et de l'interdiction de la violence[6] s'appliquent en parti-

2 Tiré de : https://www.eda.admin.ch/dam/eda/fr/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_FR.pdf
3 Cf. explications concernant l'ordonnance du 30 janvier 2019 sur la cyberdéfense militaire (OCMil ; RS 510.921), Charte des Nations Unies, projets d'articles datant de 2001 de la Commission du droit international (International Law Commission [ILC]) sur la responsabilité des États en cas d'agissements violant le droit international public (projets d'articles ILC). Ces articles ressortent en grande partie au droit international coutumier.
4 Cf. art. 2, ch. 1, de la Charte des Nations Unies.
5 Découlant de l'art. 2, ch. 1, de la Charte des Nations Unies et du droit international coutumier.
6 Cf. art. 2, ch. 4, de la Charte des Nations Unies.

culier aux opérations étatiques dans le cyberespace. Le droit humanitaire international (droit des conflits armés) s'applique en outre aux conflits armés, en qualité de loi spéciale (droit coutumier et contractuel). Il doit aussi être respecté lors d'opérations intervenant dans le CYBEEM. En lien avec la conduite de la guerre, il s'agit surtout des principes de la distinction, de la prudence et de la proportionnalité. D'autres dispositions du droit international des conflits armés à caractère coutumier sont importantes aussi pour les actions dans le CYBEEM et doivent dès lors être respectées. L'interdiction de la perfidie[7] ou la protection particulière de certaines personnes et de certains objets[8] en sont quelques exemples. Dans l'étude, la mise au point, l'acquisition ou l'adoption d'une nouvelle arme, de nouveaux moyens ou d'une nouvelle méthode de guerre, il faut de plus vérifier si leur utilisation serait interdite en permanence ou sous certaines conditions par le droit humanitaire international ou d'autres règles applicables inhérentes au droit international public[9]. Cela vaut aussi pour les cyberarmes et pour les moyens et méthodes de la cyberguerre.

Lors d'actions dans le cyberespace international, de nombreuses questions se posent en termes d'application du droit à tous les échelons de conduite. À l'échelon stratégique, l'admissibilité des mesures doit être examinée sur le fond (droit international public). À l'échelon opératif, c'est le cadre légal applicable qui doit être examiné (droits de l'homme, droit humanitaire international). Enfin, à l'échelon tactique, ce sont des questions concrètes en matière d'application du droit qui doivent être clarifiées. Dans le contexte d'un conflit armé, il s'agit par exemple du devoir de distinguer les objectifs militaires légitimes (objets militaires, combattants, groupes armés, participation directe à des hostilités, etc.) ou de faire la distinction entre ruse de guerre autorisée et traîtrise interdite. Il faut à cet égard aussi assurer une certaine unité de doctrine à travers l'ensemble des espaces d'opération.

1.4 Bases et conditions-cadres

Message sur le programme de la législature 2019 à 2023

Figurant parmi les objectifs principaux du programme de la législature, la numérisation se rapporte fondamentalement à l'administration fédérale, au service public et à l'économie.

Rapport du Conseil fédéral sur la politique de sécurité de la Suisse 2021

Le rapport du Conseil fédéral sur la politique de sécurité de la Suisse 2021 demande entre autres de renforcer la protection contre les cybermenaces et de davantage axer l'armée sur les conflits hybrides.

7 Cf. art. 37 du Protocole additionnel I aux Conventions de Genève.
8 P. ex. la protection des biens culturels (art. 53 du Protocole additionnel I), des ouvrages et installations contenant des forces dangereuses (art. 56 du Protocole additionnel I) ou d'unités sanitaires (art. 12 du Protocole additionnel I).
9 Cf. art. 36 du Protocole additionnel I et art. 11 de l'ordonnance du DDPS du 26 mars 2018 sur le matériel (OMat).

Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC 2.0) 2018–2022

La SNPC a été adoptée par le Conseil fédéral et constitue actuellement la principale directive en la matière à l'échelon fédéral. Elle s'articule de la manière suivante :

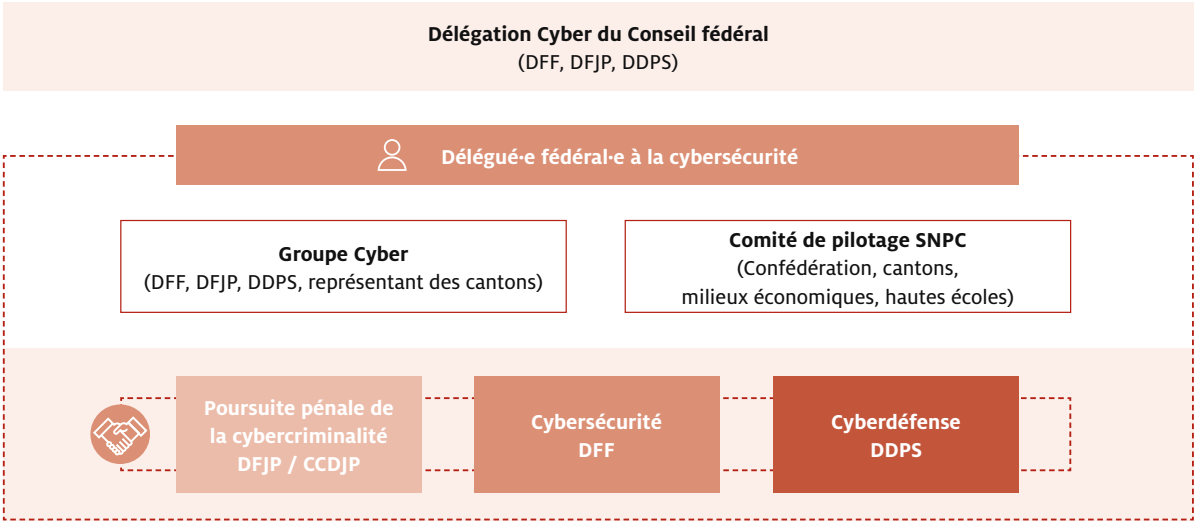


Illustration 5 : cybersécurité au sein de l'administration fédérale (Stratégie cyber du DDPS, 2021)

La conduite politique incombe à la Délégation Cyber du Conseil fédéral, présidée par le chef ou la cheffe du Département fédéral des finances. Quant au Comité de pilotage de la SNPC et au Groupe Cyber, ils sont dirigés par le/la délégué/e fédéral/e à la cybersécurité. Les trois piliers de la SNPC figurent aussi sur cette illustration, à savoir la poursuite pénale de la cybercriminalité, la cybersécurité et la cyberdéfense, et les organisations qui en sont responsables.

La SNPC contient les trois moteurs essentiels pour l'armée :

— conduite (thématique) centralisée – exécution décentralisée de la mise en œuvre (approche fédéraliste) ;
— collaboration simple et directe de tous les participants à tous les échelons nécessaires ;
— exigence vis-à-vis de l'armée de mettre à disposition ses moyens cyber à des fins d'appui subsidiaire.

Faisant intégralement partie du dispositif national global, l'armée est intégrée dans la SNPC 2.0. Les tâches qui y sont consignées sont contraignantes pour l'armée. Elles indiquent déjà une direction que la Conception générale cyber va prendre.

Stratégie informatique de la Confédération 2020–2023[10]

La stratégie informatique actuelle formule des mesures et objectifs, sur quatre axes différents. Ce qui est en premier lieu important pour l'armée, c'est le principe des prestations spécifiques et complémentaires fournies en tant que prestataire interne de la Confédération.

La Confédération s'est par ailleurs fixé comme objectif de regrouper les processus de soutien et les prestations informatiques de base. La future unité organisationnelle responsable doit ici tenir compte des exigences spécifiques de l'armée. Pour ce faire, une ordonnance propre à l'armée est planifiée dans le domaine de l'informatique (ordonnance sur l'informatique de l'armée).

10 Par suite de la décision A2021-008_B2021-031 du 4 octobre 2021 relative à la transformation numérique et gouvernance de l'informatique, ce document sera renommé en Stratégie numérique de la Confédération 2020–2023.

Stratégie Suisse numérique

La Stratégie Suisse numérique vise surtout à conserver, étendre et promouvoir les infrastructures numériques. Elle doit de plus tenir compte des aspects sécuritaires essentiels et assurer la protection contre les cyberrisques. Une étude est en cours d'élaboration à ce sujet. L'armée est concernée sur certains aspects.

Stratégie nationale pour la protection des infrastructures critiques 2018–2022

Cette stratégie définit 17 mesures par lesquelles le Conseil fédéral entend maintenir la sécurité de la Suisse en matière d'approvisionnement et l'améliorer sur certains aspects essentiels. Il a donné le mandat aux organes de surveillance et aux organes de régulation compétents de vérifier dans tous les secteurs des infrastructures critiques s'il existe des risques majeurs de perturbations graves de l'approvisionnement. Des mesures appropriées doivent permettre de réduire ces risques.

Rapports Avenir des forces terrestres et Avenir de la défense aérienne

Ces deux rapports constituent la base et le cadre du développement des forces armées pour les années à venir.

Stratégie cyber du DDPS 2021-2024

La cyberdéfense fait partie intégrante de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Le Plan d'action Cyberdéfense DDPS (PACD) datant de 2017 a défini pour la première fois les tâches, compétences et processus des unités administratives du DDPS en matière de cyberdéfense. Les mesures qui y étaient contenues ont été réalisées jusqu'à la fin 2020. La Stratégie cyber du DDPS s'appuie sur les observations faites dans le cadre du PACD. Le DDPS et ses unités administratives s'en servent pour se préparer de manière ciblée et intégrale aux exigences en la matière, en perpétuelle mutation.

L'illustration ci-dessous présente les domaines principaux du dispositif du DDPS en matière de cyberdéfense. Quatre domaines de compétence en constituent le cœur, au sein duquel la stratégie définit les objectifs concrets jusqu'à 2024, avec des champs de mesures et les cahiers des charges s'y rapportant.

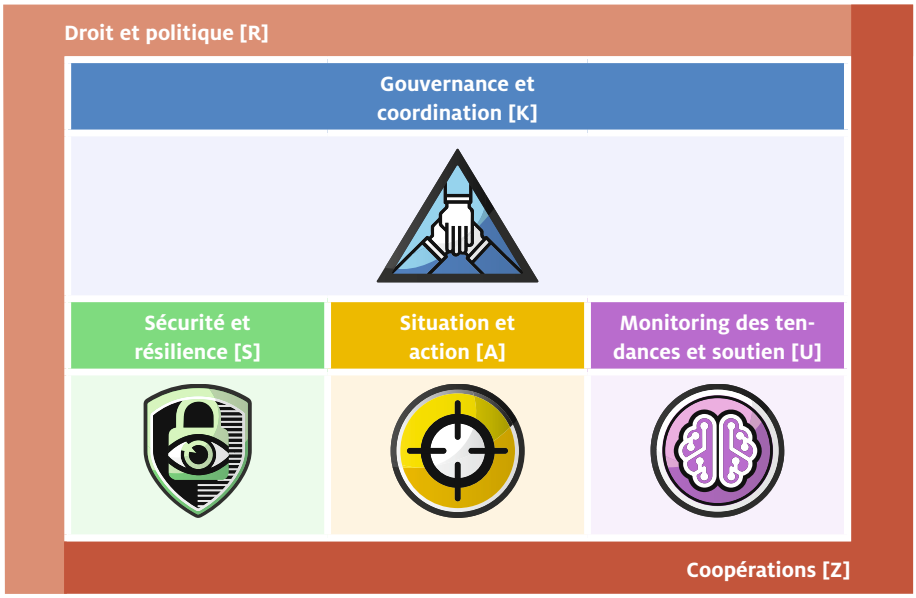


Illustration 6 : dispositif de cyberdéfense du DDPS (Stratégie cyber du DDPS, 2021)

2

Contexte et tendances d'évolution

Parallèlement à la numérisation et à l'interconnexion technique toujours plus croissante de nos sociétés, l'espace d'opération CYBEEM s'est établi comme une dimension conflictuelle supplémentaire dans les champs des politiques de pouvoir tant civiles que militaires.

La plupart des forces armées ont identifié les nouveaux défis, mais également le potentiel qui s'ouvre à elles pour mener à bien leurs actions ; elles ont ainsi mis sur pied de nouvelles capacités tant sur le plan du personnel, du matériel et des infrastructures que des performances virtuelles qu'une telle approche rend possibles.

2 Contexte et tendances d'évolution

Parallèlement à la numérisation et à l'interconnexion technique toujours plus croissante de nos sociétés, l'espace d'opération CYBEEM s'est établi comme une dimension conflictuelle supplémentaire dans les champs des politiques de pouvoir tant civiles que militaires. La plupart des forces armées ont identifié les nouveaux défis, mais également le potentiel qui s'ouvre à elles pour mener à bien leurs actions ; elles ont ainsi mis sur pied de nouvelles capacités tant sur le plan du personnel, du matériel et des infrastructures que des performances virtuelles qu'une telle approche rend possibles. Le rapport du Conseil fédéral sur la politique de sécurité 2021 souligne que l'utilisation de moyens cyber et informationnels à des fins politiques est aujourd'hui usuelle et que de plus en plus d'acteurs étatiques et non étatiques recourront vraisemblablement à ces moyens dans les années à venir. Les moyens cyber et informationnels peuvent servir à dégrader une situation en préparation à une attaque pour finalement déboucher sur un conflit armé[11]. La doctrine des différents pays montre que la mise en œuvre d'une telle approche requiert une perspective tout à la fois nouvelle et intégrale.

Les forces armées sont contraintes de constituer et maintenir les capacités CYBEEM tout en les développant en fonction des menaces. C'est un défi aujourd'hui déjà, car le CYBEEM évolue en permanence. Si des outils d'attaque tels qu'un maliciel sont par exemple découverts par la partie adverse, ils seront vraisemblablement sans effets, car les lacunes en matière de sécurité dans les systèmes cibles seront rapidement comblées. Les outils d'attaque peuvent également perdre leur effet en raison de la maintenance régulière des systèmes (p. ex. mises à jour, correction).

Un autre défi consiste à identifier comment et dans quelle direction la technologie se développe. Cette évolution doit être intégrée dans le contexte militaire afin que de nouvelles capacités puissent être mises en place.

Les systèmes informatiques, qui sont toujours plus interconnectés, ont par ailleurs besoin tous les cinq à six ans d'un renouvellement étendu, car les exigences évoluent en permanence et la durée d'utilisation du matériel et des logiciels informatiques se raccourcit de plus en plus. Les systèmes d'aujourd'hui doivent en outre répondre aux exigences actuelles en matière de sécurité et ainsi être suffisamment protégés contre les cyberattaques. Afin de raccourcir au maximum les cycles de renouvellement, il faut pouvoir disposer de processus d'acquisition, d'intégration et d'exploitation qui soient agiles et flexibles.

Tous ces aspects constituent un gros défi pour les forces armées, nécessitant de nouvelles approches, mais, plus encore, un véritable changement culturel. Pendant plusieurs décennies, l'accent a en effet été placé sur les engagements militaires classiques, avec des moyens lourds (p. ex. chars de combat) dont la durée d'utilisation s'étendait en règle générale sur plusieurs dizaines d'années. De nos jours, les systèmes informatiques doivent être renouvelés à intervalles bien plus courts. Ces exigences hautement dynamiques inhérentes aux nouveaux espaces d'opération contrastent par conséquent avec les servitudes liées aux engagements militaires classiques, plutôt axés sur des processus à long terme.

11 La politique de sécurité de la Suisse – Rapport du Conseil fédéral, état au 24 novembre 2021, p. 9

2.1 Contexte international [12]

2.1.1 De nouveaux espaces d'opération comme moyens d'exercer le pouvoir

Les nouveaux espaces d'opération sont de plus en plus utilisés pour faire valoir, voire imposer, au-dessous du seuil de conflit militaire déjà, des intérêts en matière de politique de puissance, par exemple dans le cas de tensions politiques et économiques ou de rivalités régionales ou stratégiques. Des renseignements sont notamment recherchés (p. ex. par des activités d'espionnage) dans le CYBEEM et des opérations de prise d'influence ou d'information y sont menées. En règle générale, ces actions ne sont pas isolées et les acteurs n'agissent pas non plus seuls. Au contraire des opérations cybercriminelles, les opérations d'espionnage et de prise d'influence visent dans la plupart des cas à se ménager une position avantageuse en matière de pouvoir.

Les capacités cyber étatiques sont continuellement développées à l'échelle internationale. S'y ajoutent un nombre croissant d'acteurs non étatiques agissant de manière plus ou moins professionnelle et des procédures automatisées qui évoluent en permanence créant des cybermoyens toujours plus rapides et efficaces. Les acteurs étatiques et non étatiques pratiquent l'espionnage économique et industriel de manière systématique et mènent des actions visant à influer sur les processus politiques, afin de pouvoir maintenir sa position, voire l'améliorer, au sein de la concurrence croissante de l'économie mondiale. Dans ces espaces d'opération, il n'existe que peu d'accords à l'échelle internationale pour régler les aspects juridiques et prendre les sanctions éventuelles qui s'imposent. Cela permet de dissimuler des actions et de contourner les sanctions.

Des activités d'espionnage pilotées par des États et des prises d'influence politique ont lieu dans les pays les plus divers. Celles-ci peuvent même conduire à l'oppression de sa propre population, d'opposants politiques et de groupes minoritaires à l'aide de cybermoyens, avant tout dans l'espace de l'information. La censure de canaux de réseaux sociaux, la fermeture de l'accès Internet, la propagande et d'autres opérations psychologiques en sont quelques exemples. Une étude de l'Université d'Oxford (GB) consacrée à la thématique « Global Disinformation Order » constate notamment que septante États ont mené en 2019 des campagnes organisées sur les réseaux sociaux[13].

Tendance : il faut partir du principe que

- des actions dans le CYBEEM sont menées comme moyens de la première heure sous toutes les formes de tensions interétatiques, allant de rivalités politiques et économiques jusqu'à des conflits militaires ;
- des capacités dans le CYBEEM seront à l'avenir utilisées par un nombre croissant d'États sous une forme plus ou moins étendue, afin de corroborer, défendre ou imposer des intérêts propres ;
- de plus en plus d'États de taille réduite, dotés d'un potentiel restreint en matière d'instruments, disposent de cybermoyens de surveillance très performants, dont la technologie provient de partenaires (généralement dans le cadre du renforcement des relations diplomatiques).

12 Les paragraphes qui suivent examinent l'imbrication internationale de la thématique cyber dans la politique sécuritaire, économique et de pouvoir et dans les conflits militaires. Sur le plan de la politique de sécurité, l'accent principal est mis sur l'Europe de l'Ouest et la Suisse. Les explications données s'appuient essentiellement sur les sources suivantes :
Baezner Marie, Cordey Sean (2019) : Nationale Cybersicherheitsstrategien im Vergleich – Herausforderung für die Schweiz, mars 2019, Center for Security Studies (CSS), EPFZ. Cité comme Baezner, Cordey (2019)
Dewar Robert S. : Trend Analysis : Contextualising Cyber Operations, mai 2018, Center for Security Studies (CSS), EPFZ. Cité comme Dewar (2018)
Le passage consacré aux cyberforces armées ouest-européennes s'appuie surtout sur Sean Cordey, Robert S. Dewar, éd. (2019) : National Cybersecurity and Cyberdefense Policy Snapshots : Update Collection 2, Center for Security Studies (CSS), EPFZ. Les pays suivants ont été examinés de près et un lien a si possible été établi avec la Suisse : Finlande, France, Allemagne (aussi chez Baezner, Cordey 2019) et Grande-Bretagne.

13 University of Oxford : The Global Disinformation Order : 2019 Global Inventory of Organised Social Media Manipulation (2019) ; p. 2 ss, cité comme « University of Oxford : The Global Disinformation Order (2019) »

2.1.2 Nouveaux espaces d'opération lors de conflits[14]

Lors de conflits, les États et les armées ont depuis toujours engagé les moyens les plus récents et les plus efficaces, afin de se ménager des avantages tactiques et stratégiques vis-à-vis de leurs adversaires. L'utilisation systématique et ciblée d'actions dans le CYBEEM ne constitue dès lors pas une surprise. Elles sont de nos jours utilisées comme moyens de combat usuels lors de conflits et font partie de tous les conflits modernes. De telles actions peuvent également servir à créer les conditions favorables à une attaque physique. Elles sont toutefois aussi utilisées comme ressources isolées dans le but de perturber, détruire ou déstabiliser des infrastructures et des systèmes. Afin de préparer et appuyer les actions militaires, les activités dans le CYBEEM ont souvent lieu des semaines ou des mois avant les opérations proprement dites dans les zones physiques classiques. En font notamment partie la perturbation et l'interruption de systèmes militaires et civils de communication, d'approvisionnement et de pilotage ou l'exécution de campagnes de désinformation, de propagande et de prise d'influence[15].

Le conflit entre la Russie et l'Ukraine à partir de 2014 montre de manière exemplaire à quel point un conflit militaire est souvent précédé d'un affrontement au long cours sur le plan de la politique de puissance. Les actions menées dans le CYBEEM ont là aussi joué un rôle important avant et pendant ce conflit. Les deux parties ont en effet fait un usage intensif de la désinformation et de la propagande, perturbé les télécommunications civiles, interrompu l'approvisionnement énergétique et mené des attaques à l'aide de maliciels. Dans les conflits d'aujourd'hui, de telles manières de faire font partie des procédures standard. À l'avenir, les actions dans le CYBEEM pourraient être menées à l'aide de technologies et de palettes d'outils toujours nouvelles, encore plus efficaces, auxquelles un dispositif de défense adapté devra faire face, avec un développement tout aussi rapide de contre-mesures.

Les cyberpuissances, soit les États qui disposent de cybercapacités militaires hautement développées, vont continuer à donner le ton, car elles possèdent aussi les possibilités nécessaires en termes de finances et de personnel pour concevoir et déployer des cyberarmes hautement complexes.

Les acteurs non étatiques sont un autre facteur important dans les affrontements intervenant dans le CYBEEM. Dans presque tous les conflits internationaux de ces dernières années, des groupes proches des parties en conflit ont fait parler d'eux au travers de cyberattaques. De tels groupes agissent en partie sur mandat d'un État, de leur propre chef ou pour ces deux raisons. Il faut partir du principe que des États en conflit vont engager des groupes non étatiques à l'avenir également, puisque ceux-ci disposent de capacités hautement développées et peuvent être engagés de manière ciblée pour les actions nécessaires. Ces groupes mènent souvent des cyberactions de manière inofficielle, mais bien organisée, hautement professionnelle et la plupart du temps avec des cyberoutils relativement simples, mais efficaces. Pour les États se cachant derrière ces actions, cela présente l'avantage qu'ils ne peuvent quasiment pas être identifiés comme en étant les mandants. Ils assument toutefois aussi le risque inhérent à l'absence de contrôle portant sur la conduite et les conséquences possibles de telles actions, dès qu'un groupe participe à un conflit interétatique de son propre gré.

La difficulté à retracer les actions et à identifier leurs mandants permet le plus souvent d'écarter le risque de représailles, ce qui contribue encore à réduire le seuil d'inhibition devant l'exécution de telles actions. Selon les études les plus récentes, l'évo-

14 Les conflits désignent des affrontements ouverts, internationaux ou intraétatiques, à composante militaire.

15 P. ex. le ver informatique Stuxnet (découvert en 2010) et ses évolutions. Depuis lors, aucune utilisation similaire de cyberarmes hautement développées n'a été publiquement identifiée, ce qui est probablement dû à un rapport déséquilibré entre les coûts et l'utilité. L'utilisation de telles armes ne vaut la peine que si des cibles de premier plan sont visées et exige des efforts énormes en termes de technologies, de personnel et de temps de développement. En règle générale, on préfère pour les attaques des cyberoutils qui sont peu coûteux, faciles à manier et efficaces.

lution vers une implication accrue d'acteurs non étatiques et particulièrement aussi d'acteurs isolés pourrait devenir un aspect-clé dans les futurs conflits intraétatiques[16].

Les principes classiques de la dissuasion ne sont plus immédiatement applicables dans un tel contexte diffus. Outre le fait qu'une attaque ne peut souvent pas être attribuée à un agresseur, la proportionnalité et la contrôlabilité des contre-réactions numériques ne sont pas données.

Tendance : il faut partir du principe que
- des États, des acteurs non étatiques et des individus vont mener en cas de conflits davantage d'actions étendues dans le CYBEEM, de façon anonyme et largement anticipée, afin d'influer sur la suite du conflit proprement dit ;
- les principes classiques de la dissuasion ne s'appliqueront presque plus dans le CYBEEM.

2.1.3 Stratégies en matière de cybersécurité[17]

La plupart des États occidentaux ont développé une conscience élevée pour la cybersécurité au cours des 10 à 15 années écoulées. Cela s'explique par la transformation numérique à l'échelle mondiale et les chances et les risques qui en découlent. Il en résulte nombre de stratégies nationales portant sur la cybersécurité et des concepts s'en inspirant pour la cyberdéfense militaire et policière.

Toutes les stratégies considérées ont ceci de commun qu'elles ont adopté une approche intégrale, incluant divers besoins socioéconomiques sur le plan national. Elles s'inscrivent à chaque fois dans une stratégie nationale en matière de sécurité et sont fondamentalement axées sur des cybercapacités défensives. De plus, dans toutes les stratégies, le commandement politico-stratégique dans le domaine de la cybersécurité se trouve à proximité immédiate de l'échelon gouvernemental suprême[18]. Dans toutes les stratégies examinées, la cyberdéfense est conduite séparément en fonction de son caractère militaire et civil. Celles-ci accordent une grande importance à la coopération internationale et à la collaboration avec le secteur privé et misent sur un travail complet de sensibilisation, d'information et de formation.

Dans toutes les stratégies, la question de savoir comment la cybersécurité nationale doit être assurée verticalement (à travers un pilotage efficace des ressources nationales) et horizontalement (à travers la coordination entre différents services) revêt une importance centrale. À l'échelle nationale, il faut un mélange adéquat entre centralisation et utilisation décentralisée de compétences. À l'échelle internationale, il faut définir comment la collaboration interétatique doit être aménagée. S'ajoutent d'autres champs thématiques, que les États doivent adopter. En font partie des structures solides et résistantes pour la gestion des crises, une communication efficace en cas de crises, le développement d'une bonne capacité de réaction à des incidents graves, une image appropriée de la situation et une analyse précise de la menace. La question se pose par ailleurs de savoir comment la future offre en matière de formation doit être aménagée, de sorte à pallier le manque de spécialistes dans le domaine cyber. S'agissant de la collaboration avec l'économie privée, un cadre est requis permettant des innovations et encourageant la sécurité nationale. L'harmonisation de la législation constitue par ail-

16 Dewar (2018), p. 9
17 Baezner Marie, Cordey Sean (2019) : Nationale Cybersicherheitsstrategien im Vergleich – Herausforderung für die Schweiz, mars 2019, Center for Security Studies (CSS), EPFZ. Cité comme Baezner, Cordey (2019)
18 S'agissant de l'organisation dans les différents pays, se référer à Baezner, Cordey (2019), p. 10.

leurs une thématique qui ne doit pas être sous-estimée, également dans la perspective d'une collaboration interdisciplinaire et internationale. Enfin, il faut à l'avenir des stratégies efficaces pour lutter contre la cybercriminalité.

Les principaux écarts inhérents aux exemples considérés dans le présent chapitre émanent principalement du cadre de référence historique concerné ainsi que de la culture, de l'organisation et de la structure des différents systèmes politiques. D'autres éléments distinctifs découlent du positionnement politique, de la compréhension propre et des champs d'intérêts des différents États au sein de la communauté globale des États[19].

Tendance :
- Toutes les stratégies examinées en matière de cybersécurité ont ceci de commun que la conduite nationale de la cybersécurité revêt un caractère civil, tant aujourd'hui qu'à l'avenir.
- L'utilisation du potentiel national des États va gagner en importance à l'avenir.

2.1.4 Cyberforces des grandes puissances (États-Unis, Russie et Chine)[20]

Les grandes puissances que sont les États-Unis, la Chine et la Russie disposent depuis environ deux décennies de capacités et de moyens cyber militaires efficaces pour mener des cyberactions défensives et offensives. Les structures correspondantes en matière de cybersécurité dépendent de l'évolution historique, des systèmes politiques, de la compréhension propre ainsi que des intentions et intérêts que ces États poursuivent dans le contexte global.

On peut partir du principe que les cyberforces de ces trois États sont bien alimentées en ressources personnelles et financières. La Chine pourrait même disposer de plusieurs dizaines de milliers de personnes travaillant exclusivement pour la cyberdéfense et la cyberattaque militaires. Les trois États disposent d'unités officielles propres en charge des cyberopérations militaires. Ils ont par ailleurs les capacités et moyens de fabriquer et déployer des cyberarmes hautement exigeantes[21].

Il est fortement vraisemblable que ces trois grandes puissances aient des liens plus ou moins officiels avec différents groupes non étatiques menant des actions et attaques pour leur compte. En particulier pour la Russie et la Chine, on sait que des missions étatiques sont confiées temporairement ou de manière fixe à plusieurs de ces groupes de « pirates informatiques patriotiques » et « hacktivistes ».

La connexion avec de tels groupes ou le contrôle exercé sur eux permet même d'engager des cyberforces non étatiques pour la surveillance, l'espionnage ou même le sabotage par des États. Il s'agit avant tout d'entreprises qui produisent du matériel informatique, des prestations numériques[22] et des technologies de monitorage.

Les grandes puissances mentionnées ici font de plus systématiquement usage d'opérations d'information pour faire primer leurs intérêts[23].

---

19 Cf. Baezner, Cordey (2019), p. 7.
20 Indications militaires-stratégiques : documentation PPT portant sur les cybercapacités BAC / COE / CYD (30.8.2018). L'espace électromagnétique n'est pas traité ici, par manque de sources publiquement accessibles pertinentes.
21 Cf. Baezner Marie, Robin Patrice (2017), Hotspot Analysis : Stuxnet, octobre 2017, Center for Security Studies (CSS), EPFZ.
22 Prestations telles que moteurs de recherche, produits Office, services de communication et de messagerie, réseaux sociaux, services de paiement en ligne, plateformes vidéo, achats en ligne, entreprises de cybersécurité.
23 Cf. Cordey Sean (2019), Cyber Influence Operations : An Overview and Comparative Analysis, Cyber Defence Trend Analysis, Center for Security Studies, EPFZ ; University of Oxford : The Global Disinformation Order (2019).

Tendance :
- Il faut partir du principe que les grandes puissances vont continuer à étendre et à utiliser de manière systématique leurs potentiels dans le CYBEEM et l'espace de l'information.

2.1.5 Cyberforces en Europe de l'Ouest et stratégies de cyberdéfense

Les États d'Europe de l'Ouest considérés dans le présent chapitre[24] disposent tous de cyberforces modernes au sein de leurs forces armées, dont les compétences et tâches respectives sont définies dans des stratégies de cyberdéfense. Celles-ci sont à leur tour intégrées dans des stratégies de cybersécurité supérieures ou sont pilotées en parallèle dans un cadre autonome.

Il faut souligner le fait que l'ensemble des stratégies de cybersécurité distingue très clairement la cyberdéfense militaire des tâches civiles telles que la lutte contre la cybercriminalité. Il ressort des stratégies de cybersécurité et de cyberdéfense qu'il faut une conduite centralisée tant sur le plan politique que militaire-stratégique pour coordonner des structures à l'évidence complexes. Ce poste de commandement est toujours placé à proximité de l'échelon de conduite suprême (chef de la Défense, commandement supérieur). Les pays examinés ont également constaté que la cyberdéfense militaire devait dans l'idéal être établie comme poste (de commandement) central[25]. Cette position à l'échelon de compétences le plus élevé permet au commandement des cyberforces d'agir avec des partenaires de même niveau, au sein de l'armée et à l'extérieur, de manière immédiate, par la voie de service la plus courte et d'égal à égal, tout en augmentant si nécessaire le rythme de ses actions. Parce qu'il y a tellement de parties impliquées à différents niveaux, l'exécution se fait toutefois de préférence de manière décentralisée, avec les compétences et responsabilités propres des organes exécutants lorsque c'est nécessaire.

Les cybercommandements des cyberforces d'Europe de l'Ouest s'inspirent souvent de l'organisation de commandement de l'OTAN. Les États tels que la Finlande, qui ne font certes pas partie de l'OTAN, mais qui ont des points de tangence avec elle, ont considéré la création de cyberpostes de commandement. La centralisation, structuration, conduite et surveillance de cyberforces de défense et d'attaque au sein d'un cybercommandement uniformisé selon le modèle de l'OTAN pourrait correspondre à une tendance[26].

La péjoration de la situation en matière de politique de sécurité au cours de ces dernières années a incité les forces armées à développer leurs capacités offensives. Plusieurs États ont ainsi dans un passé récent officiellement revendiqué leurs cybercapacités militaires offensives.

Toutes les forces armées disposent au minimum d'équipes informatiques d'urgence, aussi appelées Computer Emergency Response Teams (CERT). Quant aux Pays-Bas, à la France et à l'Autriche, leurs cybercapacités offensives sont avérées.

La collaboration des forces armées avec les autorités civiles, l'industrie et l'économie privée (infrastructures critiques telles que l'alimentation électrique, les télécommunications, etc.) joue un rôle déterminant dans pratiquement tous les pays, précisément

24 Baezner, Cordey (2019) : dans le cadre des stratégies nationales de cybersécurité, l'accent a aussi été mis sur l'intégration des stratégies de cyberdéfense, pour les États que sont la Finlande, la France, l'Allemagne, l'Italie et les Pays-Bas. Dans le chapitre qui suit, de possibles points communs avec la Suisse sont mis en évidence, sur la base des observations faites par Baezner, Cordey (2019). Pour les détails se rapportant aux différentes forces armées, cf. annexe.

25 Allemagne, France, Finlande, Pays-Bas, Grande-Bretagne (mis en œuvre à partir de 2020)

26 Cf. Cordey Sean, Dewar Robert S. éd. (2019) : National Cybersecurity and Cyberdefense Policy Snapshots : Updated Collection 2, 2019, Center for Security Studies (CSS), EPFZ, p. 167, point 5 ; p. 168, point 7.

aussi dans le cadre de prestations d'aide subsidiaires à des tiers ainsi que dans le domaine de la formation et de la recherche.

Une collaboration plus étroite entre organes militaires et civils peut s'observer à l'aide plusieurs exemples dans les pays examinés. On l'observe par exemple dans l'élaboration d'une image commune de la situation, dans l'échange d'informations et dans les efforts consentis en matière de sensibilisation et de conduite d'opérations communes. Afin de promouvoir une collaboration étroite et de mettre à profit les avantages inhérents à des voies d'information raccourcies, les unités cyber civiles et militaires sont dans certains pays hébergées dans les mêmes bâtiments, par exemple aux Pays-Bas[27].

Toutes les forces armées examinées soulignent l'importance de la collaboration internationale.

À l'instar des stratégies de cybersécurité, les concepts de cyberdéfense examinés se distinguent aussi avant tout par leurs toiles de fond historico-politiques respectives et par le contexte géopolitique dans lequel ils s'inscrivent.

Tendance : il s'avère que
- les cyberforces d'Europe de l'Ouest établies sont dirigées de manière centralisée et engagées de manière décentralisée ;
- d'un point de vue militaire, la collaboration avec les autorités civiles et la coopération internationale sont considérées comme importantes ;
- les effets à des fins militaires dans le CYBEEM et l'espace de l'information se produisent à l'échelon opérationnel, comme celui des effets physiques.

2.2 Contexte national

2.2.1 Politique

Comme dans de nombreux autres États, les chances et risques liés à la numérisation ont été reconnus en Suisse. Le Conseil fédéral a fixé les objectifs en la matière[28].

Parmi les nombreuses interventions parlementaires portant sur le thème de la cybersécurité, il faut mentionner en particulier deux motions qui visent le développement futur des cybercompétences de l'armée[29]. Ces deux motions poursuivent pour l'essentiel les six objectifs suivants :

1. création d'un centre de cybercompétences de la Confédération et d'un cybercommandement de l'armée pour grouper les forces et développer les cybercapacités ;
2. extension des ressources en personnel et finances pour la Confédération et l'armée ;
3. autoprotection des systèmes et infrastructures propres à l'armée et développement de capacités autonomes pour les cas de défense ;
4. appui subsidiaire ;
5. coopération entre formation, recherche, milieux scientifiques, industrie, économie et exploitants des infrastructures critiques ;
6. échanges, communication et information à l'échelon national et international.

27 Baezner, Cordey (2019), p. 10
28 Objectifs du Conseil fédéral 2020
29 Motion Eder Joachim 17.3508 (classée), Création d'un centre de compétence fédéral pour la cybersécurité
Motion Dittli Josef, 17.3507 (classée), Création d'un commandement de cyberdéfense dans l'armée suisse

La deuxième Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022 portait sur la situation dans son ensemble, au contraire de la première (2012–2017). Elle a pris en considération de nombreuses interfaces et a mieux impliqué l'armée conformément à sa mission. Elle a de plus défini de nouvelles mesures pour mieux répondre à l'état de la menace.

Tendance : il s'avère que
- l'importance de la thématique cyber est à la fois reconnue et établie dans la discussion suisse en matière de politique de sécurité ;
- des attentes politiques se font jour poussant la Suisse à renforcer ses capacités propres en la matière, afin de tenir compte des développements à l'échelle internationale.

2.2.2 Économie, formation et recherche

À l'échelle internationale, on observe diverses manières dont l'économie, la formation et la recherche collabore. L'objectif est de mettre à profit de manière systématique les avantages issus du cyberespace, de l'espace électromagnétique et de l'espace de l'information et d'améliorer dans le même temps la sécurité des infrastructures propres. Selon le pays, les institutions faisant partie de l'appareil de sécurité civil et militaire jouent un rôle différent. Indépendamment de la solution choisie, ces États visent à regrouper de manière optimale les potentiels nationaux, afin de préserver de manière aussi efficace et autonome que possible les intérêts qui s'y rapportent sur le plan de l'économie et de la sécurité.

Dans la perspective du développement et de l'utilisation de technologies-clés (cf. chap. 2.3) dans le cyberespace et l'espace électromagnétique, l'économie suisse et l'univers de la formation jouent un rôle important pour l'armée. Ils sont à la fois des moteurs importants et des fournisseurs. Et si l'armée ne veut pas être dépassée par l'évolution technologique et qu'elle souhaite utiliser les synergies, il est indispensable de mettre en place et d'encourager des partenariats et des programmes de développement communs.

Dans le domaine de la formation et de la recherche, des spécialistes sont formés en Suisse à un niveau élevé pour des métiers en lien avec le CYBEEM. Ce personnel spécialisé constitue une ressource déterminante pour l'alimentation en personnel de l'armée. L'armée soutient le secteur de la formation avec des programmes d'instruction qui lui sont propres, par exemple avec le stage de formation cyber ou la formation de base ou continue.

Tendance : il faut partir du principe que
- les coopérations nationales vont à l'avenir constituer un élément essentiel dans la formation, la recherche et l'économie, afin de renforcer et maintenir des capacités étatiques appropriées et une autonomie dans le CYBEEM et l'espace de l'information ;
- les forces armées vont encore davantage mettre à profit cette collaboration ;
- l'armée va devoir viser une collaboration nationale accrue (en partenariat) dans l'économie, la formation et la recherche. Ce sera pour elle le seul moyen d'anticiper l'évolution technologique et de recruter du personnel répondant aux défis actuels et futurs.

2.3 Le défi de l'évolution technologique

L'évolution des technologies de l'information et de la communication influe massivement sur les possibilités inhérentes au cyberespace. Les développements intéressants à cet égard s'observent aujourd'hui dans les secteurs suivants :

— augmentation de la puissance de calcul ;
— intelligence artificielle ;
— big data ;
— mise en réseau complète ;
— plateformes autonomes ;
— domination croissante de grandes firmes technologiques.

Les technologies évoluent en permanence. Ce qui était considéré comme à la pointe de la technologie il y a de cela dix ans est aujourd'hui une évidence. Les appareils qui se fondent sur une technologie ancienne sont encore largement répandus dans les systèmes TIC de l'armée, ce qui constitue un défi particulier difficile à éviter en termes de charge d'exploitation et de sécurité. Afin de préserver et renforcer les capacités ou de combler les lacunes existantes, une armée doit évoluer en permanence sur le plan technique. Elle doit obligatoirement se préoccuper des technologies, applications techniques et systèmes du futur.

Lors d'acquisitions, l'Armée suisse doit procéder à une analyse comparative entre le potentiel d'une solution technologique proposée et les risques qui y sont liés. Une éventuelle dépendance vis-à-vis de fournisseurs et de leur origine doit également être prise en considération. Les nouvelles technologies, les applications et les systèmes techniques doivent répondre aux futures capacités exigées. Ils doivent être replacés dans leur contexte global et exploités dans le cadre de la gestion intégrale du cycle de vie. En font également partie les processus ressortissants au secteur Supply Chain Risk Management, avec lesquels la sécurité d'un système est examinée sur toute sa durée d'utilisation alors que les risques passés et futurs sont eux appréciés et anticipés.

Les modifications technologiques mènent soit à des améliorations progressives ou à des sauts évolutifs majeurs, qui remplacent intégralement les anciens systèmes. Leur intégration requiert une approche flexible et interconnectée et des partenariats intensifs avec l'économie et la science. Il faut de plus des procédures d'acquisition rapides et proches des besoins liés à l'engagement ainsi que des organisations de projet flexibles.

Tendance : il faut partir du principe que

- la contrainte liée au renouvellement des systèmes va encore s'accroître en raison de l'évolution technologique galopante et que la durée d'utilisation des systèmes à haut degré de technologie va se raccourcir ;
- l'intégration d'applications et de systèmes techniques modernes va exiger une approche flexible et interconnectée, ce qui présuppose un processus d'acquisition rapide et des partenariats technologiques ciblés ;
- les systèmes du futur devront encore être examinés de manière plus approfondie quant à leur potentiel et aux risques qui y sont liés, afin que les ressources propres puissent être utilisées de façon optimale dans le cadre du portefeuille de système.

Cyberespace

Les composantes TIC telles que les smartphones et les centres de calcul sont aujourd'hui déjà souvent raccordés à des clouds. Ceux-ci enregistrent et traitent les données, sont répartis à travers la planète et fonctionnent en réseau globalisé.

Les nouveaux réseaux satellitaires (p. ex. OneWeb, Starlink) et les nouvelles méthodes de communication via satellite vont à l'avenir également amener les accès Internet dans des régions et lieux retirés, où il n'existe aucun accès terrestre à large bande. La communication par câble, par exemple via fibre optique, va par ailleurs raccorder des bâtiments à des débits de données très élevés. Les liaisons internationales seront assurées de manière encore plus redondante et avec une performance illimitée ou presque[30].

Au cours des années écoulées, diverses évolutions ont entraîné une nouvelle poussée d'innovation dans le cyberespace. En font notamment partie l'automatisation des processus économiques, la mise en réseau croissante et la disponibilité de nouvelles méthodes liées à l'intelligence artificielle et la possibilité de traiter d'immenses lots de données (big data). Sous la devise « numérisation » ou « industrie 4.0 », les interactions entre l'homme et la machine sont redéfinies. Les champs d'activité des humains se déplacent de plus en plus de tâches répétitives vers des tâches de programmation et de pilotage de processus automatisés.

Le cyberespace militaire est à maints égards à la traîne par rapport aux évolutions civiles. Il utilise dès lors souvent des technologies disponibles dans le commerce et les complète à l'aide de développements spécifiques à ses besoins. Dans le domaine des télécommunications, l'armée a en revanche besoin de procédures propres, en raison de ses exigences en matière de disponibilité, de robustesse et de sécurité, lesquelles transportent toutefois des quantités de données bien plus faibles que leurs pendants civils.

L'évolution dans le cyberespace est galopante. L'ensemble du secteur croît continuellement, tout en devenant toujours plus complexe et difficile à appréhender. La consolidation technologique repose toutefois sur des fondations qui sont conceptuellement éculées. Les technologies fondamentales n'ont pas été conçues pour de telles dimensions d'utilisation, comme la mise en réseau mondiale ou le traitement de données dans des smartphones, ordinateurs portables ou centres de données. C'est la raison pour laquelle le cyberespace est fragile sur le plan de la sécurité, puisque la sécurité intégrale est inatteignable et n'existera jamais[31].

Étant donné que le cyberespace est un espace créé par l'homme, une grande partie des risques et des menaces réside dans les activités humaines. Les cyberattaques utilisent souvent aussi les faiblesses des humains qui sont assis derrière les écrans des machines. Le cyberespace est également utilisé commercialement par une large communauté. Il en résulte en permanence de nouveaux champs, au sein desquels de nouvelles procédures et de nouveaux outils sont développés pour mener des cyberoffensives. Les meilleurs outils et processus d'attaque sont toutefois soumis à un strict maintien du secret. Ils ne s'acquièrent pas sur les marchés conventionnels.

La vulnérabilité des systèmes numériques présuppose l'existence de technologies sécuritaires correspondantes et une organisation ad hoc en la matière, en raison de l'évolution permanente des menaces. Les forces armées s'équipent en technologies de protection et d'identification toujours plus performantes. Elles forment des équipes chargées de la protection propre vis-à-vis d'assaillants. Tant les assaillants que les défenseurs utilisent des méthodes de camouflage et de tromperie. L'intelligence artificielle joue

30 Une seule fibre optique dans un câble de fibres optiques peut transporter des volumes de données de plusieurs dizaines de Tbit/s. Quant aux bâtiments situés dans les agglomérations, ils peuvent être dotés d'un débit pouvant aller jusqu'à 10 Gbit/s.
31 Des exemples tels que les faiblesses fondamentales dans les protocoles de routage d'Internet et dans l'architecture des processeurs modernes (Spectre, Meltdown) confortent ce constat.

par ailleurs toujours plus un rôle important s'agissant des technologies de protection et d'identification. La vitesse des actions intervenant dans le cyberespace est pour cette raison massivement plus grande.

Afin de conserver sa liberté d'action, l'Armée suisse doit pouvoir continuer à exister dans le cyberespace en temps de crise ou lors de conflits armés également, ce qui doit être atteint grâce à des TIC plus robustes et une séparation intelligente entre réseaux propres et publics. Contrer des activités adverses dans le cyberespace est dès lors devenu une activité militaire à plein temps, comparable par exemple avec la protection d'objets ou la défense aérienne. Si des cybercapacités offensives sont disponibles, cela peut considérablement favoriser le succès d'une action militaire. Afin d'identifier les menaces futures qui ne sont pas encore prévisibles aujourd'hui et d'engager ainsi des contre-mesures efficaces, l'armée doit aujourd'hui déjà établir des capacités propres en matière de développement technologique.

Dans le domaine militaire, il faut de plus tenir compte des aspects suivants :

— La numérisation dans le contexte militaire est une tendance irréversible. De plus en plus de systèmes autonomes seront par exemple utilisés. Cette évolution s'accompagne à la fois de chances et de risques, puisque de nouvelles opportunités se font également jour de pénétrer dans les systèmes informatiques de l'adversaire et ainsi d'entraver des processus de décision.
— Les cyberattaques peuvent par ailleurs aussi être utilisées pour transporter de fausses informations, pour provoquer de l'insécurité auprès de la population et de la troupe. Les infrastructures utilisées à cet effet ne sont la plupart du temps pas de la responsabilité de l'armée. Il est par conséquent important que l'armée collabore avec les organisations pertinentes dans le domaine. C'est la seule manière pour elle de pouvoir identifier précocement de telles attaques et de maintenir la fiabilité de ses données.
— Les systèmes militaires ne sont pas nécessairement reliés au réseau global, mais constituent parfois des réseaux dits standalone, c'est-à-dire isolés, non raccordés et limités localement. Dans un tel cas, un acteur peut tenter de pénétrer dans des systèmes informatiques locaux bien avant l'action proprement dite ou de s'en prendre à des composantes importantes en matière de sécurité, comme des appareils de télécommunication ou de cryptage. Il peut par exemple le faire lors de l'entretien d'un système. Des forces spéciales, drones miniatures, avions ou satellites peuvent également être utilisés à cet effet.

Tendance : il faut partir du principe que

- les développements techniques civils sont les forces motrices de la mise en réseau, de la transmission des données et de leur traitement ;
- les développements techniques vont conduire à un cyberespace encore plus complet, mais toujours aussi fragile ;
- les menaces non prévisibles vont en permanence mettre à l'épreuve les propres technologies en matière de sécurité, en partie développées à l'interne, ainsi que la propre organisation sur le plan de la sécurité, et exercer une pression sur elles ;
- le cyberespace militaire, en sa qualité de fragment du cyberespace dans son ensemble, ne pourra pas à l'avenir être considéré comme absolument sûr et sera exposé à des tentatives d'attaque permanentes ;
- le taux de succès des actions militaires peut être augmenté grâce à des cybercapacités offensives propres ;
- la nécessité de protéger à l'aide de moyens appropriés des plateformes d'armes autonomes et des réseaux isolés, par exemple des systèmes d'armes autonomes, va augmenter.

Données et informations

Le succès d'une action militaire est déterminé par le déploiement de forces appropriées (p. ex. une formation militaire ou un avion de combat) au bon endroit et au bon moment. Afin de pouvoir le planifier et piloter, le commandant responsable doit disposer à temps des informations nécessaires à cet effet (image de la situation). L'importance des informations était particulièrement élevée et l'est encore, particulièrement dans le contexte militaire[32]. En raison de l'évolution technologique, la quantité d'informations a nettement augmenté. Il y a de plus en plus d'informations à disposition sur un contexte donné et les modifications y interviennent rapidement. Si la difficulté était par le passé d'accéder aux informations nécessaires, le défi consiste aujourd'hui à distinguer les informations importantes parmi la grande quantité de données existantes.

Afin de pouvoir visualiser les observations importantes dans une image de la situation, il faut une analyse aussi continue que possible de ces données. Les résultats alimentent directement la planification des actions, les données et les informations ainsi rassemblées constituant le cœur de la numérisation du processus de conduite de l'action.

Les tendances dans ce domaine englobent :

— l'amélioration de la qualité et l'augmentation de la vitesse dans la conduite de l'action à travers des données de qualité, pertinentes et disponibles au même moment pour toutes les parties impliquées, dans le but d'appuyer le déploiement précis des moyens limités ;
— la facilitation de la collaboration à travers des bases, une langue et une doctrine communes ;
— l'évitement d'un trop-plein d'informations ;
— le maintien de l'intégrité des informations et des données.

L'homme, la cybersécurité et les TIC jouent un rôle central, ces dernières jouant le rôle de porteuses des données. Elles mettent à disposition la logique et la prestation de traitement nécessaires et permettent l'échange de données. Il y a par ailleurs besoin d'une culture encourageant le partage d'informations et la collaboration. Dans le même temps, les données qui nous appartiennent doivent être protégées. Les mots-clés à cet égard sont ici confidentialité, intégrité et disponibilité des données ainsi qu'authenticité, caractère contraignant, fiabilité et résilience. Des règles sont définies dans le cadre de la gestion de l'information, lesquelles sont respectées par toutes les parties impliquées et appuyées par les TIC.

S'agissant de la conduite des futurs engagements militaires, les informations numériques constituent un facteur-clé du succès au-delà des frontières des organisations et systèmes. La disponibilité des données nécessaires est par ailleurs un facteur critique. Il dépend directement du succès dans la lutte pour obtenir des informations à l'avance, de l'autoprotection dans le domaine cyber et de la conduite d'exploitation TIC. En termes simplifiés, cet avantage signifie qu'une partie a un niveau de connaissance plus avancé sur un contexte donné qu'une autre.

La législation portant sur la sécurité de l'information et la protection des données joue un rôle important à cet égard. Étant donné que des règles différentes sont souvent valables dans les secteurs ressortissants à la gouvernance et que des conventions (relations de confiance) y font défaut, les partenaires devraient régler leurs relations en matière d'échanges de données dans des accords. Chaque organisation impliquée conserve toutefois dans ce contexte la souveraineté sur les informations et les données dans le champ de compétences qui lui incombe. Elle décide donc seule quelles sont les informations qu'elle partage avec qui.

32 Les effets dans l'espace de l'information, p. ex. dans le cadre d'opérations de l'armée, ne font pas partie de la présente conception générale. Ceux-ci sont décrits dans les bases servant d'orientation à long terme de l'armée.

Tendance : il faut partir du principe que

- l'échange d'informations va gagner en importance et que son efficacité va dépendre d'un comportement humain adéquat et d'une culture de collaboration ;
- la conduite de l'action va s'accompagner de flux de données variables fortement interconnectés et d'un grand flot de données, qui vont exiger une priorisation et l'engagement d'une logique d'information ;
- la collaboration avec des partenaires externes va augmenter, ce qui va aboutir à un espace d'information flexible, extensible et fédéré, au sein duquel des accords de collaboration (gouvernance et relations de confiance) seront exigés.

Espace électromagnétique

L'espace électromagnétique permet la communication de données sans câble entre deux ou plusieurs composantes de systèmes informatiques, la localisation et le pilotage d'appareils tels que des drones aériens ou des engins explosifs. Grâce à l'indépendance vis-à-vis des conduites physiques (p. ex. les câbles), l'espace électromagnétique offre une variété de possibilités d'utilisation peu coûteuses, rapidement applicables et géographiquement flexibles. Pour la conduite mobile de formations et de systèmes militaires sur le terrain ou dans les airs, la communication de données par radio[33] est la seule technologie utilisable.

L'Armée suisse utilise un nombre croissant de systèmes radio différents avec des technologies variées. Leur cycle de vie et la gestion de leur sécurité représentent un défi, surtout que la technique radio utilisée est souvent déterminée par le fabricant d'un système d'armes. Dans le contexte de l'armée, ce sont avant tout des systèmes radio à rayonnements dirigés (faisceaux hertziens) et non dirigés (p. ex. appareils radio tactiques) électromagnétiques qui sont utilisés, dans les gammes de fréquences et types de signaux les plus variés. L'armée utilise par ailleurs davantage des Software Defined Radios (SDR), grâce auxquels une partie des fonctions d'un émetteur ou récepteur radio sont assurées par des logiciels (numérisés). Les SDR peuvent en règle générale être administrés de manière centralisée et peuvent très bien devenir des cibles de cyberattaques, en leur qualité de « petits ordinateurs ».

Les équipements et technologies nécessaires pour mener des actions dans l'espace électromagnétique dépendent des systèmes qu'il faut explorer et combattre. À chaque fois que de nouveaux signaux ou de nouvelles procédures servant à la transmission d'informations sont utilisés, il faut aussi consolider techniquement les systèmes inhérents à l'exploration et à la perturbation électroniques. Si cela n'est pas le cas, ces systèmes vont selon les circonstances perdre complètement leur efficacité en très peu de temps[34]. D'où l'importance de saisir et d'analyser en permanence les nouveaux signaux et les nouvelles procédures dans le spectre électromagnétique (exploration électronique) et d'observer constamment l'évolution sur le plan de la technique radio.

Le « combat électronique » va également à l'avenir servir à identifier des systèmes radio, de radar et de navigation satellite adverses au sol et dans les airs, à les localiser et à limiter voire supprimer intégralement leur fonctionnalité par des contre-mesures

33 Technique radio : « Sous-domaine de la technique de renseignement englobant tous les processus et appareils techniques servant à la transmission sans câble de signaux à l'aide d'ondes radio », définition traduite du Duden, https://www.duden.de/rechtschreibung/Funktechnik

34 Il est p. ex. imaginable qu'une partie adverse implémente peu avant une attaque des signaux et des processus nouveaux et inconnus sur ses systèmes radio (Software Defined Radio) et rende ainsi inefficaces les systèmes électroniques d'exploration et de perturbation. À l'inverse, cela signifierait que l'Armée suisse utiliserait en temps de paix d'autres signaux et processus radio qu'en cas de conflit.

électroniques. Dans le même temps, il faut soustraire les propres systèmes radio à une exploration adverse et protéger les propres systèmes d'exploration et de perturbation. Des actions visant à impacter les systèmes d'exploration électronique adverses peuvent aussi être menées à cet effet[35].

Les armes dites à haute énergie constituent un sous-groupe de systèmes d'armes porteur d'avenir dans l'espace électromagnétique. Il s'agit d'une nouvelle génération de moyens d'action qui utilisent de l'énergie combinée. Ils sont utilisés dans le contexte militaire pour mettre hors de combat, endommager, désactiver ou encore détruire des équipements, des installations et du personnel adverses. Ils sont utilisés dans de nombreux secteurs et deviennent de plus en plus performants grâce à l'évolution technologie continue. Les armes à champ magnétique, les canons à plasma, les armes à ultrasons et les armes à rayonnement électromagnétique (laser à haute énergie ou armes éblouissantes) sont des exemples de telles armes. Ces dernières revêtent de l'importance pour la présente conception.

Dans l'espace électromagnétique, les systèmes d'exploration et de perturbation électroniques avec leurs capteurs et moyens d'action ainsi que les centrales d'opération attenantes disposent d'un propre réseau intégré de capteurs, de renseignement, de conduite et d'action (CRCA). Celui-ci est à son tour intégré dans la zone des effets du réseau de conduite supérieur de l'armée. Dans le futur environnement des signaux, il faudra bien plus de capteurs, puisqu'une saisie ne sera plus possible qu'à partir d'un secteur relativement proche, ceci en raison des caractéristiques modernes des signaux. Cette tendance vaut en principe aussi pour les moyens d'action. En raison du nombre élevé de signaux radio émis ainsi que de la performance des capteurs et des moyens d'action, le volume de données est très élevé dans l'espace électromagnétique. Il est probable que dans un proche avenir seules les technologies modernes telles que l'intelligence artificielle ou la Big Data Analytics soient encore en mesure d'interpréter des informations utiles dans un délai raisonnable. L'interface entre homme et machine va de plus devoir changer, par exemple via la réalité augmentée. C'est la seule façon pour l'armée de suivre le rythme opérationnel au sein du CRCA et de traiter des données complexes suffisamment rapidement.

Les conflits hybrides et le fait que l'armée interviendrait en cas de conflit probablement en terrain bâti exigent une plus grande flexibilité dans les configurations techniques et les capacités des systèmes. D'un point de vue militaire, elles devraient être en mesure de saisir et combattre aussi les systèmes radio civils utilisés par la partie adverse. Dans le contexte opérationnel d'aujourd'hui, il faut de petits systèmes d'exploration et de perturbation électroniques, partiellement portatifs, qui peuvent s'intégrer facilement et rapidement dans un système d'ensemble plus large. Cela devrait permettre aussi de développer la capacité des combattre des Improvised Explosive Devices (IED) à l'aide de contre-mesures électroniques. La capacité de lutter contre de tels explosifs existe certes aujourd'hui déjà de manière rudimentaire dans le secteur du déminage et de l'élimination de munitions non explosées (DEMUNEX), mais elle n'est actuellement planifiée et utilisée ni de façon interconnectée ni dans le cadre d'une opération globale.

35 Assurent l'utilisation propre de l'espace électromagnétique en dépit de la conduite adverse de la guerre électronique, comme partie du combat électronique. Elles englobent des mesures actives et passives.

Tendance : il faut partir du principe que

- les systèmes nécessaires à la saisie et à l'action dans l'espace électromagnétique devront être exploités de manière permanente et être continuellement développés sur la base de nouveaux scénarios de menaces ;
- des acteurs vont agir sur l'ensemble du spectre dans l'espace électromagnétique (également non militaire) afin d'atteindre leurs objectifs, sans tenir compte des régulations suisses ;
- le combat électronique avec des capteurs et effecteurs dégradables, axés sur les buts et interconnectés, sera utilisé tout en étant mené à l'échelon de l'armée à l'aide de la conduite en réseau intégré CRCA, à travers l'ensemble des espaces d'opération existants ;
- des effets combinés à travers l'ensemble des espaces d'opération existants vont améliorer durablement et efficacement l'appui au combat ;
- le facteur temps combiné à des volumes de données élevés va exiger l'utilisation de nouvelles technologies (science des données) ;
- l'interface entre l'homme et la machine va évoluer de la simple place de travail informatique vers une plateforme d'interaction multidimensionnelle (réalité augmentée).

Technologies de l'information et de la communication

Les technologies de l'information et de la communication (TIC) sont présentes dans tous les secteurs d'activités de la société et constituent ainsi le cyberespace. Au vu de leur transversalité, elles influent massivement sur les possibilités au sein du CYBEEM. Les TIC traitent des informations en permanence, dirigent des systèmes, préviennent de dangers et permettent aux hommes et aux machines de communiquer ensemble.

Les éléments moteurs du développement des TIC sont les suivants[36] :

— capacité de dégradation (fonctionnement de composants TIC séparés ou de parties entières de réseaux), décentralisation, numérisation, besoin permanent en liaison et échange d'informations ;
— modularisation, intégration, fédération, coopération, standardisation, automatisation et technologies ;
— cybermenaces croissantes, sécurité de l'information, intérêts nationaux, lois, démographie et situations juridiques.

Afin que des informations fiables soient disponibles, un appui TIC effectif et efficient est déterminant.

La mise à disposition quasiment simultanée et géographiquement indépendante d'informations rendant tout simplement possible la supériorité visée en la matière est un champ d'action important des TIC. D'autres champs d'action sont l'accélération des processus (hausse de l'efficacité) et l'automatisation de processus répétitifs (traitement de données en masse). Grâce à de récents développements d'algorithmes, les commandants militaires peuvent par exemple utiliser aujourd'hui déjà des simulations et formes d'intelligence artificielle pour préparer leurs décisions.

36 Ils découlent de l'architecture TIC 4.0, où ils sont précisés.

Afin que l'armée puisse préparer les données nécessaires à l'engagement, une mise en réseau intégrale est indispensable pour l'échange d'informations. Une telle mise en réseau doit à tout moment fonctionner de manière sûre et robuste. Les prérequis à la sécurité et à la robustesse sont une gestion uniforme de l'information, une standardisation des processus et des données et la définition de l'architecture en matière de sécurité.

L'armée doit être en mesure de co-déterminer l'application des TIC à l'aide de mesures correspondantes sur le plan organisationnel et législatif. Les étapes nécessaires qui mènent au succès dans l'utilisation des TIC doivent être définies dans des processus propres. Pour que les TIC puissent fournir leurs prestations sans accrocs et de manière durable, une large automatisation est nécessaire, aussi bien dans la conduite de l'exploitation TIC que dans l'exploitation TIC.

Afin de combler les éventuelles lacunes dans les prestations informatiques fournies par l'armée ou aussi relier des systèmes en silo isolés, il est possible d'utiliser des moyens de télécommunications civils en complémentarité.

Tendance : il faut partir du principe que

- la saisie, le traitement, l'enregistrement et la diffusion de quantités de données toujours plus grandes vont exiger des technologies adéquates et des processus d'automatisation et de standardisation ;
- la mise à disposition concertée, automatisée et à temps d'informations sur la base des besoins des utilisateurs génère une supériorité sur le plan de l'information et donne donc l'avantage recherché du point de vue de la prise de décision ;
- les futures TIC devront être indépendantes d'un lieu, dégradables, modularisées et standardisées, afin de pouvoir couvrir les besoins axés sur les utilisateurs et utilisatrices ;
- la gestion des technologies, à savoir les technologies et leur maniement, va être l'un des facteurs-clés de succès des futures TIC en lien avec l'automatisation et la numérisation ;
- les TIC nécessitent des prestations de support automatisées étendues, qui doivent au moins partiellement être compatibles avec les besoins de milice ;
- l'exploitation des TIC doit être hautement sécurisée, robuste et redondante, en raison des effets exercés par la partie adverse, ceci à l'échelle de l'armée dans son ensemble et jusqu'à l'échelon tactique inférieur.

Cryptologie

La cryptologie est le seul moyen de conserver et de transmettre des données en toute sécurité. Celle-ci joue donc un rôle central au sein du CYBEEM. La cryptologie traite de la conception, de la construction et de l'analyse de systèmes d'information sûrs. Elle fait la distinction entre les notions de cryptographie et de cryptanalyse.

S'agissant de la cryptographie, il s'agit de la réalisation de cryptosystèmes sécurisés. Les principaux buts de protection dans la cryptographie sont la confidentialité, l'intégrité, l'authenticité et le caractère contraignant. Un cryptosystème donné ne doit pas nécessairement remplir tous ces objectifs.

De l'autre côté, on retrouve la cryptanalyse. Elle vise à casser des cryptosystèmes et donc à compromettre leur sécurité, par exemple en pénétrant de manière illégale dans des systèmes d'ordinateurs, en les espionnant ou en manipulant des données. L'armée peut utiliser à son profit la cryptanalyse lors de tensions et de conflits, comme moyen offensif. Au quotidien, elle est surtout utilisée pour l'exploration, par exemple de renseignements cryptés.

Dans le cadre de l'évolution technologique du futur, les grands ordinateurs quantiques universels vont jouer un rôle important. À l'heure actuelle, beaucoup d'énergie est mise à travers le monde dans la recherche et le développement qui s'y rapportent. Au contraire des ordinateurs usuels, ces ordinateurs quantiques ne travaillent pas sur la base de la physique classique, mais sur la base d'états quantummécaniques. Grâce à eux, il pourrait être possible à l'avenir de briser quelques-uns des algorithmes de chiffrage les plus connus et les procédés d'échange de codes. À l'heure actuelle, quelques problèmes de fond doivent encore être résolus dans le domaine de leur développement, comme les taux d'erreur élevés et la décohérence (modifications irréversibles dues aux interactions). D'où la difficulté de pronostiquer avec précision le moment où des ordinateurs quantiques à même de servir à commettre des attaques contre des procédés cryptographiques courants seront disponibles.

Dans le domaine de la sécurité de l'information, les composantes cryptographiques (p. ex. systèmes de traitement de données) sont omniprésentes. Elles peuvent notamment protéger efficacement des informations et des systèmes. La complexité des systèmes de traitement de données a toutefois tellement augmenté que les procédés cryptographiques standardisés ne sont plus un garant de sécurité.

Trois caractéristiques constituent les principaux prérequis permettant à la cryptographie de protéger efficacement un système :

1. Un concept d'engagement cryptographique, car les algorithmes cryptographiques les plus sûrs ne servent à rien s'ils sont mal utilisés d'un point de vue conceptuel.
2. L'exécution correcte des fonctions cryptographiques : de petites erreurs dans l'implémentation suffisent déjà à provoquer des conséquences fatales.
3. Une intégrité protégée pendant toute la durée d'utilisation. C'est la seule manière d'appliquer correctement les fonctions cryptographiques.

Pour un État ou une armée, il est dès lors crucial de disposer de compétences cryptographiques propres. Il serait extrêmement risqué en effet de se reposer uniquement sur les compétences techniques d'autres États ou organisations données.

La cryptographie et la cryptanalyse sont interdépendantes et sont développées ensemble, car plus les systèmes cryptographiques ont été examinés à l'aulne de capacités et d'instruments cryptanalytiques, plus ils sont efficaces. À l'inverse, la cryptanalyse profite du savoir-faire de la cryptographie, quand les concepts cryptographiques peuvent être impliqués dans l'analyse. C'est la raison pour laquelle le potentiel dans ce domaine ne peut être complètement utilisé qu'à travers la combinaison des deux compétences.

Tendance : il faut partir du principe que

- les fonctions cryptographiques vont de plus en plus être intégrées dans les solutions logicielles et matérielles ;
- les évolutions techniques futures vont rendre inutilisables certains procédés isolés de cryptage ;
- seules les compétences cryptographiques propres et la gestion des fonctions cryptographiques techniques vont offrir la sécurité requise ;
- grâce à la cryptographie et à la cryptanalyse, les systèmes propres futurs pourront être examinés et protégés efficacement ;
- la cryptographie et la cryptanalyse se complètent et ne peuvent déployer leur plein potentiel que si elles sont combinées.

2.4 Observations

Afin que l'armée puisse s'acquitter de ses tâches[37], elle doit pouvoir opérer de manière intégrale sur l'ensemble des espaces d'opération. La prestation-clé de l'armée dans le CYBEEM consiste à mettre à disposition des informations et des services de ses propres TIC, indépendamment d'un lieu, et à les protéger. Ce faisant, elle ne doit pas mettre en péril les partenaires reliés et ainsi assurer sa propre capacité et celle de ses partenaires en matière de conduite dans toutes les situations. Et comme les cyberattaques sont quotidiennes, l'armée doit pouvoir assurer cette protection en permanence, soit au quotidien également. Elle doit par ailleurs être capable d'appuyer des opérations et engagements militaires dans d'autres espaces d'opération à travers des actions dans le cyberespace et l'espace électromagnétique[38]. Les activités dites cyber electromagnetic activities (CEMA) permettent à cet égard de prendre des mesures efficaces jusqu'à l'échelon tactique, afin d'obtenir la supériorité en matière de savoir[39].

Éléments moteurs émanant des bases conceptuelles existantes[40]

Les bases conceptuelles existantes permettent en résumé de déduire cinq éléments moteurs fondamentaux :

— Premièrement, l'accent est mis sur la capacité à collaborer avec des partenaires sur le plan technique et procédural, cette collaboration étant organisée de manière fédéraliste.
— Deuxièmement, l'exigence de numérisation est présente dans l'ensemble des concepts examinés, sans toutefois que la notion de « numérisation » soit définie précisément en relation avec l'armée.
— Troisièmement, l'importance nationale de la protection contre les cyberrisques est sans cesse soulignée au sein de l'armée également.
— Quatrièmement, la SNPC et ses trois piliers que sont la poursuite pénale de la cybercriminalité, la cybersécurité et la cyberdéfense intègrent l'armée dans le dispositif national en matière cyber en lui confiant des tâches concrètes. Trois exigences posées à l'armée revêtent une importance centrale à cet égard, à savoir se protéger soi-même, collaborer avec des partenaires civils et appuyer subsidiairement les autorités.

37 Protéger et défendre la Suisse ainsi que sa population, appuyer subsidiairement les autorités civiles en cas de besoin, préserver la souveraineté aérienne et contribuer à la promotion de la paix.
38 Cf. chap. 5 consacré aux capacités.
39 UK Ministry of Defence, Joint Doctrine Note 1/18, Cyber and Electromagnetic Activities, 2018
40 Cf. chap. 1 Introduction : message sur le programme de la législature 2019 à 2023 ; rapport du Conseil fédéral sur la politique de sécurité de la Suisse 2016 ; Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC 2.0) 2018–2022 ; Stratégie informatique de la Confédération 2020–2023 ; Stratégie Suisse numérique ; rapports Avenir des forces terrestres et Avenir de la défense aérienne ; Stratégie cyber 2020 du DDPS ; objectifs de la BAC 2022, orientation de l'armée à long terme.

— Cinquièmement, à l'instar des rapports Avenir des forces terrestres et Avenir de la défense aérienne, les concepts concernant l'orientation de l'armée à long terme exigent la mise en place d'une conduite en réseau digitale entre tous les échelons de conduite.

CYBEEM en opération et à l'engagement

La prestation requise ne peut pas seulement être fournie en cas de tensions ou de conflits, mais elle doit être disponible au quotidien déjà, où les cyberattaques se déroulent anonymes et affranchies de toutes contingences de lieu. Cet état de fait influe considérablement sur la manière dont les éléments opérationnels et les capacités requises sont aménagés. À l'engagement, des systèmes informatiques isolés localement limités et non reliés (systèmes stand-alone) peuvent être attaqués par des CEMA adverses et ne peuvent dans le pire des cas plus remplir leur mission. Or on ne tient aujourd'hui pas suffisamment compte de cette nouvelle « dimension » des influences adverses sur les systèmes propres. Afin d'empêcher une compromission de ses systèmes par des cyberattaques et de pouvoir mener également des cyberactions offensives propres, l'armée devra à l'avenir protéger ses systèmes de manière permanente.

L'armée doit répondre aux exigences liées à la fois au soutien et aux menaces. Elle doit pouvoir fournir ses prestations dans le CYBEEM de manière permanente, dégradable, évolutive, modulaire et interconnectée, ceci en fonction de la mission, indépendamment d'un lieu, dans toutes les situations et à travers l'ensemble des espaces d'opération.

Mise en réseau nationale

L'armée est au quotidien déjà très étroitement interconnectée sur le plan national. Il est attendu d'elle qu'elle soit en mesure de se protéger durablement elle-même dans le CYBEEM et qu'elle ne devienne pas un risque sécuritaire national. L'interconnexion technique croissante avec des partenaires civils exige par ailleurs des standards communs, entre autres afin que l'armée puisse bien appréhender les développements au niveau civil (technologies, droit, processus, etc.). Une interconnexion étroite peut avoir des effets facilitants ou limitatifs. C'est pourquoi il est important que l'armée puisse accompagner et co-construire cet environnement. Elle doit de plus trouver les possibilités lui permettant de mieux utiliser le potentiel en relation avec le savoir-faire, les technologies, les forces de travail, etc.

Société et politique

On retrouve au centre des préoccupations l'exigence politique selon laquelle l'armée doit s'attaquer efficacement à la thématique de la cyberdéfense. Elle doit se protéger elle-même et prendre de manière autonome des cybermesures en cas de nécessité de se défendre. Il est de plus exigé que l'armée implique activement la milice dans les tâches cyber.

En fin de compte, l'armée doit également pouvoir se protéger contre la cybercriminalité, qui utilise en partie des outils hautement développés. Elle doit aussi éviter que ses systèmes soient détournés de leur usage premier pour des actions illégales.

Technologies

Les technologies et les systèmes dans le CYBEEM évoluent rapidement et constamment. Dans ce contexte, les développements technologiques civils constituent les forces motrices de la mise en réseau, de la transmission des données et de leur traitement intelligent. Ils mènent à un cyberespace croissant, mais aussi fragile. Si la vitesse de développement est tellement élevée, c'est parce que la demande globale issue de la société et de l'économie vis-à-vis de solutions nouvelles est toujours plus élevée. L'organisation s'y rapportant en matière de sécurité subit des avancées en continu et se retrouve sous pression. Elle doit s'adapter aux nouvelles menaces et remplacer les anciennes technologies de sécurité.

Les composantes informatiques des nouveaux biens d'armement se fondent souvent sur des technologies et des systèmes nouveaux ou améliorés. Ces dernières ne sont pas la seule raison pour laquelle l'Armée suisse doit régulièrement adapter ses systèmes informatiques. Les technologies existantes obsolètes ne peuvent plus non plus remplir les nouvelles exigences militaires. Les grands groupes technologiques dictent indirectement à l'armée les matériels et les logiciels dont elle peut disposer sur le marché et les composantes qu'elle doit remplacer. L'évolution technologique CYBEEM dans l'armée est donc fortement conditionnée par des influences externes. Pour l'armée, il est donc indispensable de pouvoir suivre ces évolutions, pour qu'elle mette à profit les chances qui en découlent et identifier précocement les dangers et les risques qui y sont liés. À cette fin, l'armée a besoin d'une gestion de la technologie et d'un portefeuille technologique qui lui permettent de recourir à temps à des technologies modernes et de fournir les prestations d'appui exigées de manière automatisée. L'objectif est de mettre à disposition des informations en fonction des besoins de clients, en temps opportun et de manière automatisée, afin de générer une supériorité en matière d'information et d'amener l'avantage visé en termes de prise de décision. Afin de garantir les capacités-clés CYBEEM, les technologies modernes doivent être acquises et rendues utilisables rapidement.

Contexte international

L'image de conflit décrite dans le chapitre 2.1 met en évidence le fait que les actions menées dans le CYBEEM sont plus fréquentes dans tous les conflits contemporains et qu'il va de soi qu'elles sont utilisées comme moyens de puissance. Dans ce domaine, on assiste également à une évolution et à une consolidation permanentes de ces moyens. Les actions CYBEEM interviennent souvent de manière très anticipée, c'est-à-dire en temps de paix déjà, avant le conflit proprement dit.

Afin que l'armée puisse accomplir ses tâches, elle doit pouvoir fournir ses prestations de manière coordonnée dans tous les espaces d'opération, aussi bien lors de tensions marquées qu'en cas de conflits. La protection permanente vis-à-vis des cybermenaces au quotidien déjà est la condition préalable nécessaire à cet effet.

Les diverses stratégies de cyberdéfense d'autres forces armées ne constituent pas des éléments moteurs directs pour l'Armée suisse. Elles montrent toutefois que les impacts dans le CYBEEM devraient en principe être regroupés au sein d'une seule et même organisation et orchestrés à l'échelon opératif.

3

Bases organisationnelles et légales

La définition de dispositions légales pour le développement dans le CYBEEM requiert la connaissance du développement organisationnel et de ses conditions-cadres légales.

3 Bases organisationnelles et légales

3.1 Introduction

Conformément à l'art. 5 de la Constitution (Cst.), le droit est la base et la limite de l'activité de l'État. Celle-ci doit répondre à un intérêt public et être proportionnée au but visé[41].

La Constitution fixe par ailleurs les tâches de l'Armée suisse. L'armée contribue à prévenir la guerre et à maintenir la paix ; elle assure la défense du pays et de sa population. Elle apporte son soutien aux autorités civiles lorsqu'elles doivent faire face à une grave menace pesant sur la sécurité intérieure ou à d'autres situations d'exception. La loi peut prévoir d'autres tâches[42].

Les lignes qui suivent montrent comment les structures organisationnelles actuelles sont nées au sein de l'administration militaire et de l'armée et comment les données y sont traitées[43]. Les structures organisationnelles et leurs bases légales sont un miroir du contexte et des évolutions sociétales et politiques de leur temps, les modifications futures étant toujours dépendantes de ces dernières ou en découlant.

Les structures déterminent à leur tour les services spécialisés au sein de l'administration fédérale qui doivent fournir telles et telles prestations ainsi que la manière avec laquelle les autres services peuvent y recourir.

S'agissant des prestations fournies dans le CYBEEM et de l'exploitation de systèmes informatiques, ce constat vaut sans exception aucune. Seule la considération des structures et évolutions dans ces domaines de manière ex post permet d'appréhender les conditions-cadres existantes et d'identifier les défis qu'il s'agira de relever pour répondre aux besoins futurs.

3.2 Développements organisationnels

3.2.1 Prestations en matière de renseignement

En 2008, l'Assemblée fédérale a chargé le Conseil fédéral de subordonner au même département les deux services qui remplissaient des missions de renseignement civil[44]. C'est ainsi qu'est né le Service de renseignement de la Confédération (SRC) en 2010, à partir des unités de renseignement du Service d'analyse et de prévention (SAP) du Département fédéral de justice et police (DFJP) et du Service de renseignement stratégique (SRS) du DDPS. Il se fonde aujourd'hui sur la loi fédérale du 25 septembre 2015 sur le renseignement (LRens : RS 121)[45]. Les bases légales appliquées jusque-là pour le SRS et le SAP ont pour leur part été abrogées[46]. Avant ce regroupement, le SRS était responsable de la recherche d'informations à l'étranger et de leur analyse, le SAP s'occupant lui du service de renseignement intérieur[47]. Pour ce dernier, cette responsabilité découlait de

41 Art. 5, al. 1 et 2, Cst.
42 Art. 58, al. 2, Cst. Les autres tâches figurent à l'art. 1 LAAM.
43 Cf. l'art. 3, let. e, de la loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1), qui définit le traitement des données personnelles comme toute opération effectuée indépendamment des moyens et procédés utilisés, notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données.
44 Art. 2 de la loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC, abrogée)
45 Cf. message du 19 février 2014 concernant la loi sur le renseignement (FF 2014 2030, ci-après message LRens).
46 Cf. annexe I LRens (RO 2017 4134).
47 Cf. Système d'interception des communications par satellites du Département fédéral de la défense, de la protection de la population et des sports (projet « Onyx »). Rapport de la Délégation des commissions de gestion des Chambres fédérales du 10 novembre 2003, FF 2004 1377, chap. 4.2, p. 1389 (ci-après projet « Onyx ») ; Lutter plus efficacement contre le terrorisme et le crime organisé. Rapport du Conseil fédéral du 9 juin 2006 donnant suite au postulat du 21 février 2005 de la Commission de la politique de sécurité du Conseil des États (05.3006), FF 2006 5421, chap. 3.2.2, p. 5436.

la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI). La responsabilité du SRS reposait, elle, sur l'art. 99, al. 1, de la loi du 3 février 1995 sur l'armée (LAAM), état au 1er janvier 2004. Cette dernière a été complétée par l'ordonnance du 4 décembre 2000 sur le renseignement (ORens ; RS 510.291)[48].

En 2004, l'armée a mis en service le système d'interception des communications par satellites « Onyx ». Cette nouvelle capacité en matière d'exploration satellitaire a signifié une intervention dans les droits fondamentaux, qui a exigé une adaptation des bases légales ad hoc. L'entrée en vigueur de l'ordonnance du 17 octobre 2012 sur la guerre électronique et l'exploration radio (OGE)[49] en a découlé[50]. Sur le plan technique[51], la capacité de procéder à l'exploration satellitaire a été développée dans la Division de la conduite de la guerre électronique (CGE)[52]. La LAAM et l'OGE définissaient qu'il n'était généralement pas permis de transmettre au SRS des informations concernant la Suisse[53], puisque celui-ci n'avait pas le droit de procéder à des activités d'exploration dans le pays[54].

Outre l'exploration radio, l'exploration du réseau câblé[55] a aussi à la suite été effectuée par le Centre des opérations électroniques (COE, autrefois BAC-CGE / division CGE), car seul celui-ci est autorisé à disposer des infrastructures techniques nécessaires[56]. En décidant que le COE ne serait pas directement lié au bénéficiaire des prestations, le législateur a voulu protéger les droits fondamentaux[57]. Dans l'exploration du réseau câblé, certains flux de données sont interceptés sur des câbles de télécommunication internationaux et, comme pour l'exploration radio, ils sont examinés, triés et exploités selon leur contenu. Contrairement à la surveillance des télécommunications en Suisse, qui est une mesure de recherche soumise à autorisation[58], l'exploration du réseau câblé est un instrument de recherche d'informations à l'étranger, lui aussi soumis à autorisation[59].

Afin d'utiliser efficacement le peu de ressources disponibles, le SRC a consciemment renoncé lors de la mise en œuvre de la LRens à constituer une expertise qui existait déjà auprès du service d'exécution COE. C'est la raison pour laquelle ce dernier est à chaque fois mandaté par le SRC pour exécuter des mesures de recherche soumises à autorisation selon l'art. 26, al. 1, let. d, et art. 37 LRens et infiltrer des systèmes et réseaux informatiques. L'infiltration est effectuée dans le but de rechercher les informations que ces systèmes et réseaux contiennent ou de perturber, empêcher ou ralentir l'accès à des informations.

48 L'ordonnance définissait que le Renseignement stratégique gérait « les activités de renseignement permanentes en rapport avec l'étranger ».
49 Entrée en vigueur le 1er novembre 2012.
50 Cf. Légalité et efficacité du système d'exploration radio « Onyx ». Rapport de la Délégation des commissions de gestion des Chambres fédérales du 9 novembre 2007, FF 2008 2293, chap. 5.5.1, p. 2305.
51 Cf. projet « Onyx », chap. 4.4, p. 1391.
52 Un service du Groupe de l'aide au commandement de l'État-major général.
53 Le SRC a pu mandater la division CGE comme prestataire technique pour les missions d'exploration sur la base de la législation militaire (cf. bases juridiques de l'exploration électronique de la Confédération du 24 avril 2003, Office fédéral de la justice, 3, p. 6s.).
54 Cf. le projet « Onyx », chap. 4.2, p. 1390.
55 Cf. message LRens, chap. 1.3, p. 2102 : « Au cours de ces dernières années, avec l'élargissement des réseaux très performants de fibre optique, les télécommunications passent de plus en plus de moyens sans câble (radio) à des réseaux reliés par des conduites (appelées ci-après « câble » par souci d'intelligibilité). Parallèlement, les possibilités d'obtenir des résultats à partir de l'exploration radio diminuent quelque peu. »
56 Cf. message LRens, chap. 1.3, p. 2101.
57 Cf. message LRens, chap. 1.3, p. 2102-2103.
58 Les mesures soumises à autorisation sont des recherches effectuées en Suisse qui ne peuvent pas être exécutées de son propre chef par le SRC ; cf. art. 26, al. 1, let. b, art. 38 LRens.
59 Cf. art. 39 ss LRens.

3.2.2 La sécurité militaire selon l'art. 100 LAAM

Les capacités de l'armée en matière de renseignement sont définies dans la LAAM et se distinguent de celles du service pour la sécurité militaire[60]. Dans le message du 8 septembre 1993 relatif à la LAAM[61] (chap. 3, p. 104), le Conseil fédéral indique qu'« il est prévu de séparer de manière stricte le service de sécurité militaire et le service de renseignements militaires, mais aussi de créer un cloisonnement entre les services de l'armée et le contre-espionnage, éventuellement le service de renseignements civils, tout en réglant de manière précise l'échange des informations entre ces services » et que « grâce à cette séparation, il sera possible de mieux définir et attribuer les tâches et les compétences de chaque service ». Avec cette séparation, le législateur a clairement établi que le service de sécurité militaire n'avait pas à remplir de tâches de renseignement en situation ordinaire[62]. Ses tâches consistaient à apprécier la situation en matière de sécurité et à protéger des ouvrages et des informations militaires[63].

Avec le développement de l'armée, le législateur a également conservé la séparation entre le Renseignement militaire (RM) et la Sécurité militaire[64]. Dans le cadre de la modification de la LAAM du 18 mars 2016, il a notamment[65] créé la base nécessaire à la cyberdéfense militaire, à l'art. 100, al. 1, let. c, LAAM[66]. De la sorte, l'obligation a été confiée au DDPS de combattre les cyberattaques visant les systèmes et les réseaux militaires à l'aide de mesures appropriées[67]. Avec l'ordonnance du 30 janvier 2019 sur la cyberdéfense militaire (OCMil), l'ordonnance d'exécution de l'art. 100, al. 1, let. c, LAAM est entrée en vigueur au 1er mars 2019[68].

Les structures actuelles sont par la suite pour la plupart apparues politiquement. Les organes mentionnés se trouvent au sein du SRC et du Groupement D du DDPS. En sa qualité de service de renseignement, le SRC a la mission de rechercher des informations et de les traiter, afin de préserver les intérêts nationaux importants (art. 2, en relation avec les art. 3 et 6 LRens). Au sein du Groupement Défense, le COE est subordonné à la BAC. En sa qualité de service exécutant, il assure sa mission sur la base de la LRens et de la LAAM.

3.2.3 Capacité en matière de capteurs

Service de renseignement civil

Le COE fournit des prestations dans le domaine de l'acquisition de données issues du renseignement en matière de communication au profit du SRC et sur ses ordres. Le COE traite des données qui ont été saisies dans le cadre de missions d'exploration radio et d'exploration du réseau câblé et les met à la disposition du SRC pour analyse.

---

60 Le service pour la sécurité militaire était réglé à l'art. 105 LAAM (1993). Il était compétent pour l'appréciation de la situation en matière de sécurité militaire, la protection d'informations et d'ouvrages militaires, l'exécution de tâches dans le domaine de la police criminelle et de la police de sécurité dans le domaine de l'armée, les mesures visant à assurer la sécurité préventive de l'armée à l'égard de l'espionnage, du sabotage et d'autres actions illicites. Il recherchait des renseignements lorsque ses membres étaient convoqués à un service actif ou un service d'appui et assurait la protection des membres du Conseil fédéral, du chancelier de la Confédération et d'autres personnes, lorsque ses membres sont mis sur pied pour un service d'appui ou un service actif. Avec la révision de la LAAM du 1er janvier 2018, certaines tâches du service pour la sécurité militaire ont été reprises au sein du DDPS par la Police militaire et le Service de protection préventive de l'armée (SPPA).

61 Message du 8 septembre 1993 relatif à la loi fédérale sur l'armée et l'administration militaire et à l'arrêté fédéral sur l'organisation de l'armée, FF 1993 IV 1

62 Cf. message LAAM 1993, chap. 3, p. 106 : « Ce n'est pas la tâche des organes de sécurité militaire en temps de paix de faire de la recherche de renseignements actives ; cette tâche ne fait pas partie de l'appréciation de la situation en matière de sécurité. »

63 Cf. message LAAM 1993, chap. 3, p. 106.

64 Cf. message du 3 septembre 2014 relatif à la modification des bases légales concernant le développement de l'armée, FF 2014 6757.

65 L'ordonnance du 21 novembre 2018 sur la sécurité militaire (OSM) s'appuie également sur l'art. 100 LAAM. L'ordonnance indique les nouveaux points forts, en plus de la création du RM et du SPPA.

66 L'art. 100, al. 1, let. c, LAAM n'était pas prévu dans le projet du Conseil fédéral. La norme n'a été introduite sous sa forme actuelle que lors des débats parlementaires. C'est la raison pour laquelle il n'existe pas de matériaux pouvant être consultés sur cette norme.

67 Cf. conseiller aux États Kuprecht et conseiller fédéral Maurer, BO 2015 E 708.

68 L'ordonnance règle les mesures à prendre en situation normale dans le domaine de la cyberdéfense concernant l'autoprotection et l'autodéfense de l'armée et de l'administration militaire en cas d'attaque contre leurs systèmes d'information et leurs réseaux informatiques (cf. ordonnance sur la cyberdéfense militaire, commentaire des dispositions, p. 1).

Le COE a mis en place des capacités dans le domaine de l'exploration radio et de l'exploration du réseau câblé ainsi que de la recherche d'informations dans des systèmes et réseaux informatiques étrangers, afin qu'il soit en mesure de remplir sa mission[69]. Les bases légales nécessaires se trouvent à l'art. 26, al. 1, let. d, ch. 1, LRens et à l'art. 37, al. 2, LRens pour la recherche d'informations dans des systèmes et réseaux informations de tiers, à l'art. 38 LRens pour l'exploration radio et aux art. 39 ss LRens pour l'exploration du réseau câblé.

Renseignement militaire (RM)

Le RM est autorisé (art. 99, al. 1bis, LAAM) à confier des missions d'exploration radio conformément à l'art. 38 LRens. Ces missions sont exécutées par le COE, indépendamment des missions du SRC. Le RM dispose en plus de l'exploration radio stratégique, conformément à l'art. 99, al. 1ter, LAAM.

3.2.4 Efficacité

Efficacité sur le plan du renseignement

Sur ordre du SRC, le COE peut infiltrer des systèmes et des réseaux informatiques tiers, afin de perturber, d'empêcher ou de ralentir l'accès à des informations (art. 26, al. 1, let. d, ch. 2, et 37, al. 1, LRens). Lorsque la cible se trouve en Suisse, ces mesures doivent être autorisées par le Tribunal administratif fédéral et validées par la cheffe ou le chef du DDPS, après consultation de la cheffe ou du chef du DFAE et du DFJP (art. 26, al. 1, let. d, ch. 2, LRens). Si la cible est située à l'étranger, l'aval du Conseil fédéral est nécessaire (art. 37, al. 1, LRens). Elles n'entrent en ligne de compte qu'en cas d'attaques contre des infrastructures critiques.

Toute décision politique de mener une opération militaire, que ce soit en temps de paix, de tension ou de conflit se fonde sur l'ensemble des consignes entrant en ligne de compte (concernant p. ex. l'aviation civile) et sur toutes les conséquences pour la population civile, l'économie et l'administration fédérale.

Efficacité sur le plan militaire

Les actions de perturbation du spectre électromagnétique[70] et la guerre électronique (GE) s'effectuent par le COE et la brigade d'aide au commandement 41 (br aide cdmt 41). Ce qui est important, c'est que l'armée ne peut entraver de manière autonome que les fréquences militaires. Si elle veut perturber des fréquences civiles, également dans la zone de sécurité d'installations militaires protégées, elle a en situation normale besoin de l'approbation de la cheffe ou du chef du DDPS[71].

Sur ordre de la BAC, le COE peut pénétrer dans des systèmes et des réseaux informatiques de tiers, afin d'empêcher des cyberattaques contre des systèmes et réseaux propres en situation normale, grâce au concours de personnel de l'administration militaire (art. 100, al. 1, let. c, LAAM, en relation avec l'art. 2, al. 1, OCMil). L'autorisation à cet effet est donnée par le Conseil fédéral[72].

3.2.5 Infrastructure

La base nécessaire à l'ensemble des capacités dans le contexte du renseignement et dans le contexte militaire est l'infrastructure[73]. Avec la mise en place de ces capacités,

---

69 La délimitation territoriale n'est pas importante pour la qualification.

70 Le spectre électromagnétique englobe par principe la totalité des ondes électromagnétiques de différentes longueurs d'ondes, c'est-à-dire d'ondes radio au rayonnement gamma en passant par le rayonnement infrarouge (rayonnement thermique) et la lumière visible. La délimitation entre fréquences militaires et civiles est réglée dans le plan national d'attribution des fréquences.

71 Art. 12 OGE

72 L'autorisation pour une telle mesure est donnée par le Conseil fédéral (art. 7 OCMil).

73 L'exploitation de l'infrastructure, indépendamment de l'état de développement, exige du personnel hautement qualifié. C'est la raison pour laquelle les directives de la Confédération doivent être respectées s'agissant des capacités en matière de recrutement et de promotion du personnel.

des infrastructures numérisées correspondantes sont également créées et exploitées. Les nouveaux systèmes liés aux capacités sont toujours intégrés dans un système global. Leur protection[74] doit être garantie en tout temps. L'exploitation des divers systèmes repose sur différentes bases légales, non reliées[75]. Celles-ci définissent à chaque fois l'accès au système, l'autorisation de traiter des données et le but de ce traitement.

3.2.6 Poursuite pénale militaire

La poursuite pénale de la cybercriminalité incombe aux autorités de poursuite pénale ordinaires et militaires. La justice militaire est compétente lorsqu'un auteur présumé a violé le code pénal militaire du 13 juin 1927 (CPM) et est ainsi soumis à la juridiction militaire. Les civils peuvent également être soumis au CPM pour certaines infractions, par exemple en cas d'acte de sabotage au sens de l'art. 86a CPM. Les violations portant exclusivement sur des dispositions en vigueur du code pénal (CP) tombent dans le champ de responsabilité des autorités de poursuite pénale ordinaires. S'il y a dans le même temps des violations contre des dispositions du CPM et aussi du CP, les autorités de poursuite pénale militaires et ordinaires coordonnent leur procédure. Elles passent en règle générale un accord, afin que l'ensemble de la procédure puisse être menée par une seule autorité pénale.

3.3 Bases légales existantes

3.3.1 Traitement de données

Le traitement de données est devenu indissociable de l'action militaire et du travail quotidien au sein de l'administration militaire. Le traitement des données personnelles doit toujours reposer sur une base légale[76]. Sans traiter de données à l'aide de moyens informatiques à travers des réseaux et des systèmes, l'armée ne peut ni s'acquitter de ses tâches quotidiennes ni planifier et mener des opérations militaires. Les bases légales précisent quelles sont les données et les informations qui peuvent être échangées avec quel partenaire sur quel système[77]. Concrètement, on utilise des systèmes pour le traitement de données avec des partenaires nationaux et internationaux et on détermine la conservation et l'effacement de ces données. Ce n'est qu'à ce moment-là que les données peuvent être traitées, de sorte qu'une alliance de systèmes et de réseaux puisse voir le jour. Outre la possibilité fondamentale d'échanger des données, celles-ci doivent être catégorisées à la fois par l'expéditeur et le destinataire. C'est à cette fin qu'il existe des accords sur la protection et l'échange de données avec des partenaires internationaux[78].

Le contexte numérique exerce une grande influence sur le travail au sein de l'armée. C'est la raison pour laquelle il faut réguler à la fois les systèmes et les réseaux[79] à utiliser et les procédures administratives[80]. Les systèmes et les programmes spécifiques, par exemple pour la gestion des affaires, sont soumis à des prescriptions qui définissent leur maniement et les conditions-cadres s'y rapportant[81]. Les données sont partout et

---

74 La protection comme capacité découle indirectement de l'OCMil. Il existe par ailleurs des bases qui chargent le chef de la BAC de protéger les systèmes et les réseaux militaires. La capacité à protéger des systèmes englobe diverses autres capacités, p. ex. en matière cryptanalytique.

75 Les systèmes sont par ailleurs délimités par le cercle d'utilisateurs, p. ex. SIC FT et SIC FA.

76 Art. 5, al. 1, et 36, al. 1, Cst. ; art. 6, al. 1, et 34, al. 1, nLPD

77 Loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée (LSIA ; RS 510.91) ; ordonnance du 16 décembre 2009 sur les systèmes d'information de l'armée (OSIAr ; RS 510.911)

78 À la fin juin 2021, neuf accords portant sur l'échange et la protection d'informations classifiées existaient avec différents pays européens. Il existe par ailleurs d'autres conventions spécifiques, par exemple avec l'OTAN (Federated Mission Networking, FMN).

79 P. ex. par l'ordonnance du 16 août 2017 sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération (OSIS-SRC ; RS 121.2).

80 P. ex. l'ordonnance du 8 septembre 1999 sur l'archivage (OLAr ; RS 152.11)

81 P. ex. l'ordonnance GEVER du 3 avril 2019

elles sont utilisées par l'ensemble de la société. Leur traitement repose sur des règles du droit fédéral que l'administration militaire et l'armée sont tenues de respecter[82].

Une attention particulière est accordée à la transmission de données via des ondes radio[83]. Comme mentionné plus haut, une partie des plages de fréquences disponibles en Suisse sont attribuées à l'armée. L'utilisation et la régulation de cette plage de fréquences incombent à la seule responsabilité de l'armée[84]. La plus grande partie des fréquences disponibles en Suisse sont toutefois civiles et non militaires. Des services de télécommunication[85] doivent être proposés à la population et à l'économie à travers ces fréquences. Les fréquences sont attribuées aux soumissionnaires de services de télécommunication à l'aide de concessions et sont dès lors strictement régulées. Un soumissionnaire ne peut utiliser que la fréquence qui lui a été attribuée. S'il en utilise d'autres, il est sanctionné en conséquence par l'organe compétent[86].

3.3.2 Organisation

L'organisation des départements et des offices fédéraux découle principalement de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA) et de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA). Ces bases sont valables pour l'ensemble de l'administration fédérale et à travers tous les départements et les offices fédéraux, indépendamment de leurs tâches, compétences et aménagements.

Les objectifs, fonctions et tâches spécifiques des différents offices fédéraux sont consignés dans des ordonnances d'organisation sur la base des objectifs des départements concernés. Pour le DDPS, ils sont définis dans l'ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (Org-DDPS ; RS 172.214.1).

En tant qu'organisation, l'armée ne fait pas partie de l'administration fédérale, mais constitue une organisation étatique en tant que telle. Elle constitue dès lors une sorte de « cas particulier ». Son organisation est réglée dans des actes juridiques propres. Ces actes sont les suivants : la Constitution (art. 58, al. 1, et 60, al. 1), la loi du 3 février 1995 sur l'armée (LAAM, titre sixième Organisation de l'armée), l'Organisation de l'armée du 18 mars 2016 (OOrgA), ordonnance du 29 mars 2017 sur les structures de l'armée (OStrA) et ordonnance du DDPS du 29 mars 2017 sur l'organisation détaillée de l'armée (OODA).

Les structures organisationnelles de l'administration militaire et de l'armée sont en partie identiques. Il y a ainsi dans les deux structures un état-major de l'armée, un commandement des opérations, une base logistique de l'armée, une base d'aide au commandement et un commandement de l'instruction. Les offices fédéraux du Groupement Défense ne fournissent pas seulement des prestations pour l'administration fédérale et l'armée. Ils doivent également pouvoir les mettre subsidiairement à la disposition de tiers, par exemple d'organisations à feux bleus[87]. Ils doivent de plus pouvoir assurer l'échange nécessaire d'informations et de données dans le contexte international. Pour être en mesure de fournir ces prestations, il faut des bases techniques et légales correspondantes. Dans ce contexte, le spectre du traitement des données doit être appréhendé de manière intégrale.

82 P. ex. la loi fédérale sur la protection des données et la loi sur la sécurité de l'information (LSI), dont l'entrée en vigueur est prévue en 2023
83 S'agissant du spectre électromagnétique, cf. le chapitre consacré à l'efficacité sur le plan militaire.
84 Art. 22, al. 4, de la loi du 30 avril 1997 sur les télécommunications (LTC ; RS 784.10)
85 Art. 3, let. b, LTC : transmission d'informations pour le compte de tiers au moyen de techniques de télécommunication
86 Art. 49 ss LTC
87 Cf. l'art. 67 LAAM Service d'appui en faveur des autorités civiles (subsidiarité).

3.3.3 Exigences législatives

Les tâches constitutionnelles de l'armée sont le point de départ de la législation s'y rapportant. Des actes normatifs tels que la loi fédérale sur la protection des données (LPD) et la loi sur les télécommunications (LTC) déterminent par ailleurs le cadre dans lequel l'armée peut développer ses capacités. Il doit être dans l'intérêt des bénéficiaires de prestations d'aménager les conditions-cadres légales de telle manière à ce que l'armée puisse y conserver sa liberté de manœuvre.

Les tâches de l'armée sont complexes. Pour la législation, c'est à chaque fois un défi que de garantir à temps les bases légales correspondantes. L'architecture TIC 4.0 du 9 mai 2020 de la BAC constate par exemple que l'alliance des systèmes constitue aujourd'hui et demain le principal défi à relever. Grâce à cette alliance, des données[88] peuvent être échangées et mises à disposition entre différents bénéficiaires de prestations et partenaires, sans perte de temps et indépendamment de toute contrainte géographique. Or, avec chaque nouveau partenaire civil, le système global à surveiller et à protéger s'agrandit[89]. Il en résulte de nouveaux points faibles et de nouvelles exigences posées à l'égard de la vitesse de transmission des données et des mesures de protection[90]. Des aspects dont il s'agira de tenir compte également dans les futures réglementations.

On peut déduire des explications fournies au chapitre 1.3 que les données doivent être mises à disposition en fonction de la mission et des capacités existantes. Le cadre légal devra à l'avenir être aménagé de manière à ce que les données ou les observations qui en sont tirées en lien avec un mandat confié au profit d'un bénéficiaire de prestations puissent être utilisées dans d'autres buts. Il faut par ailleurs qu'il y ait une transparence des données à différentes fins qui ont été mises en place en parallèle au sein de différents organes[91].

3.4 Perspectives

Le déploiement de capacités et leur exploitation doivent être assurés par les bases légales existantes ou par des modifications législatives, sachant que le développement des capacités découle de l'analyse du mandat légal et du cadre de la réglementation. L'alliance des capacités, des partenaires et des systèmes ainsi que la collaboration et l'interconnexion étroites entre administration militaire et armée doit mener à des bases légales harmonisées, voire uniformisées. Il faut ainsi éviter autant que faire se peut les réglementations divergentes[92].

Au vu des bases légales existantes, le traitement des données n'est aujourd'hui possible que de manière restreinte, alors que celui-ci constitue une capacité centrale, avec le concours de tous les impacts qui en découlent sur les systèmes et les réseaux. Les tâches sont à ce point complexes que le traitement ne se fait pas seulement au sein de l'administration fédérale, mais également sur le plan fédéral et en dehors, avec des partenaires nationaux et internationaux. Il faut donc créer les bases légales nécessaires.

S'agissant des capacités de l'armée, il faut des bases légales étendues et spécifiques. Si elles ne sont pas actualisées en permanence, l'utilisation de capacités à tout moment et dans toutes les situations est mise en péril ou n'est plus possible que pour une durée limitée.

---

88 Il s'agit de données techniques et non de données personnelles, qui servent p. ex. à suivre la situation ou à analyser des programmes.

89 Les partenaires ne se trouvent pas seulement au sein de l'administration fédérale (p. ex. OFPP et OFIT), mais aussi en dehors, dans le secteur organisé sur la base du droit privé (p. ex. RUAG SA).

90 On citera ici à titre d'exemple la problématique de la classification et des normes de sécurité non uniformes.

91 GE de l'armée et GE des Forces aériennes. Les deux capacités s'appuient sur l'OGE, mais il existe toutefois deux directives indépendantes. La directive GE de l'armée ne prévoit aucun échange de données, au contraire de la directive GE des FA (directives valables jusqu'au 31.12.2023).

92 L'alliance des systèmes fait que les infrastructures civiles sont utilisées militairement tous les jours. En cas de conflit armé, l'infrastructure civile utilisée militairement devient donc un but militaire légitime.

Il s'agit dès lors de surveiller étroitement les interdépendances et les développements et de modifier les bases légales correspondantes lorsque c'est nécessaire, afin que l'armée soit en mesure de répondre à l'ensemble de ses besoins en termes d'organisation et de capacités[93].

Les bases légales doivent être mises à jour et complétées à l'avance, pour des raisons liées à l'État de droit. Pour exécuter une mission, il faut d'abord que les dispositions légales nécessaires soient en vigueur. Dans le cadre des travaux à venir, il faudra toujours garder en tête si des bases légales doivent être adaptées ou créées pour la réalisation de la présente conception générale et, si c'est le cas, lancer le processus à temps.

93 On renvoie ici à titre d'exemple à la révision de la LAAM et de l'OOrgA. Seules ces bases permettent de modifier d'une part la structure et l'articulation de l'armée et d'autre part sa mission.

4

Doctrine

À l'engagement, le vainqueur est celui qui prend le plus rapidement la bonne décision, se donnant ainsi une longueur d'avance. Pour l'Armée suisse, il s'agit donc de prendre l'avantage en matière de connaissances et de décisions, et de le conserver – cela, déjà au quotidien.

4 Doctrine

Par doctrine, on entend tous les principes généraux selon lesquels l'armée s'acquitte de ses tâches dans le but d'atteindre les objectifs fixés en termes de politique de sécurité et de stratégie militaire, aussi bien au quotidien que dans les situations de tension accrue et de conflit. Les menaces et les risques auxquels la doctrine doit donner des réponses aussi dans le CYBEEM, servent de point de référence à cet effet.

4.1 Introduction

4.1.1 Cadre opératoire

Les actions dans le CYBEEM ne peuvent pas être considérées isolément. L'armée mène ses engagements dans tous les espaces, c'est-à-dire pas uniquement dans le cyberespace et dans l'espace électromagnétique, mais en particulier aussi au sol et dans les airs. Elle utilise par ailleurs des applications spatiales (p. ex. pour la navigation de précision et la recherche de renseignements) et prend en compte l'espace de l'information. Pour qu'une armée puisse atteindre ses objectifs stratégiques et opératifs, les actions militaires doivent être exécutées dans tous les espaces simultanément. Ces actions menées dans les divers espaces se complètent, se renforcent et se substituent mutuellement dans leur efficacité. Le commandement des Opérations conserve la vue d'ensemble à l'échelon supérieur ; il assure le suivi de la situation sur le plan global et il coordonne l'ensemble des actions militaires dans tous les espaces d'opération.

4.1.2 CYBEEM

Ce qui est essentiel à la réussite de tout engagement militaire, c'est la cohérence opérationnelle, c'est-à-dire la synchronisation et la coordination spatio-temporelles des effets et actions des formations militaires dans tous les espaces d'opération. En sa qualité d'interface entre les espaces de l'information et les espaces physiques que sont le sol, les airs, les mers et le spatial, le CYBEEM joue un rôle important à cet égard. C'est en effet en son sein que sont traitées les données et les informations utiles à la planification et à la conduite des engagements avant d'être transmises sans délai entre formations et systèmes. C'est par ailleurs en son sein aussi que la conduite adverse peut être entravée, par exemple à travers la perturbation ou l'interruption des transmissions de données de l'adversaire ou encore la paralysie de systèmes d'information de conduite.

Pour que les systèmes militaires puissent produire un effet, ils ont pratiquement sans exception tous besoin des TIC. Par exemple, un char n'est pas seulement un système d'armes dont le canon permet de combattre des buts terrestres, mais il est également relié au cyberespace à travers les TIC implantées en son sein. De plus, si la transmission de données se fait sans câble, il est également relié avec l'espace électromagnétique. Cette mise en réseau revêt notamment une grande importance pour la transmission des données, la recherche de renseignements ou encore le combat électronique contre les systèmes radio.

4.2 Confidentialité, intégrité et disponibilité des données et des informations dans le CYBEEM

Trois points d'ancrage revêtent une importance centrale pour l'ensemble des actions dans le CYBEEM, à savoir la confidentialité, l'intégrité et la disponibilité des données et des informations. Ils sont importants à la fois pour la protection propre et pour les actions offensives et relevant du service de renseignement.

1. Attaques visant la **confidentialité** (confidentiality) : lorsque des données sont enregistrées, transmises et traitées, leur confidentialité doit être garantie à tout moment. Cela n'est possible que si personne ne peut accéder sans autorisation à des informations dans un système. Les attaques contre la confidentialité peuvent intervenir aussi bien dans l'espace électromagnétique (p. ex. lors de l'exploration radio) que dans le cyberespace.

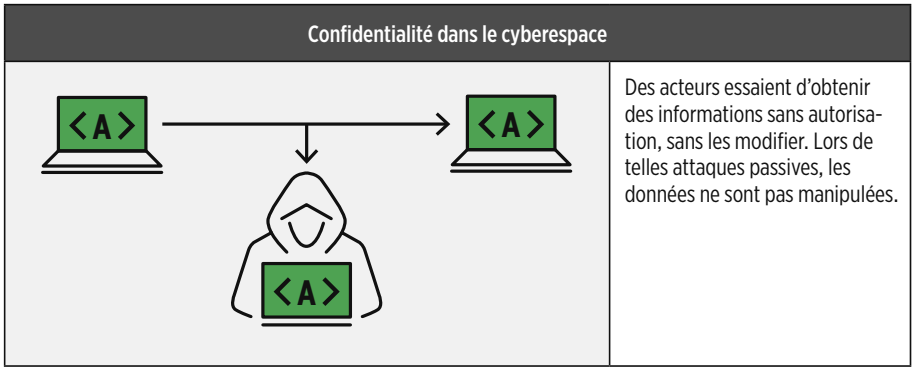


Illustration 7 : principe d'une attaque visant la confidentialité dans le cyberespace

Dans l'espace électromagnétique, les informations confidentielles ne peuvent être recherchées que pendant une durée limitée, à savoir lorsqu'elles sont diffusées via des ondes radio. Contrairement à ce qui est le cas pour les cyberattaques, il est impossible de pénétrer dans des systèmes avec les seuls moyens de l'exploration radio pour y rechercher des informations confidentielles. En revanche, il est relativement facile de trouver des informations autres à l'aide d'actions dans l'espace électromagnétique, en détectant par exemple l'emplacement d'un émetteur à l'aide de la localisation radio.

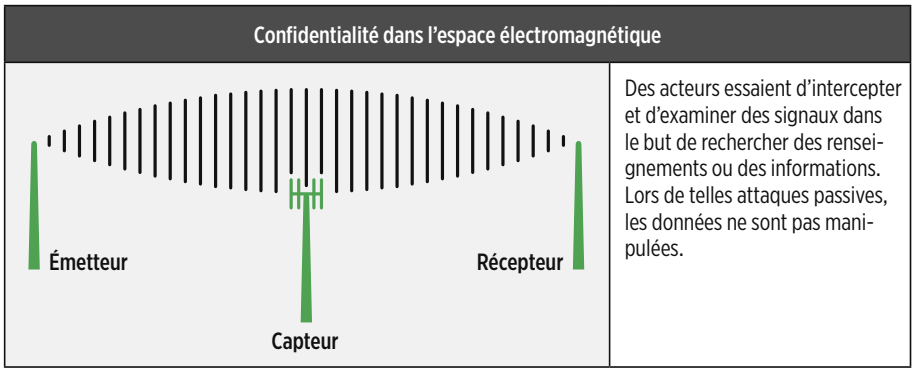


Illustration 8 : principe d'une attaque visant la confidentialité dans l'espace électromagnétique

2. Attaques visant l'**intégrité** (integrity) : L'intégrité des données est garantie lorsque celles-ci ne peuvent être modifiées de manière non autorisée ou discrète. Toutes les modifications doivent pouvoir être retracées. Ce principe s'applique principalement au cyberespace.

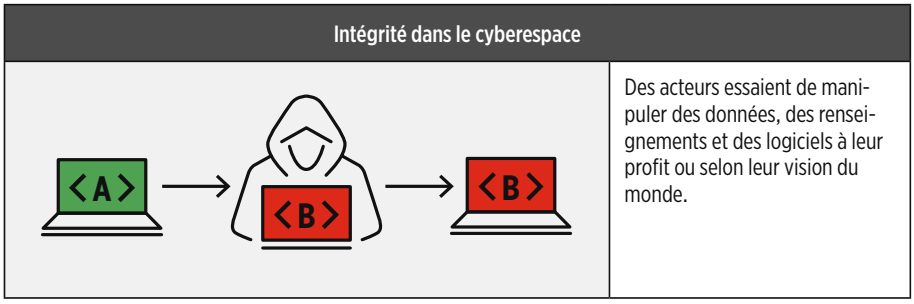


Illustration 9 : principe d'une attaque visant l'intégrité dans le cyberespace

3. Attaques visant la **disponibilité** (availability) : un système garantit la disponibilité lorsque l'accès aux données est authentifié et autorisé, et que celles-ci et les services peuvent être utilisés avec la qualité requise, sans délai et sans perturbation.

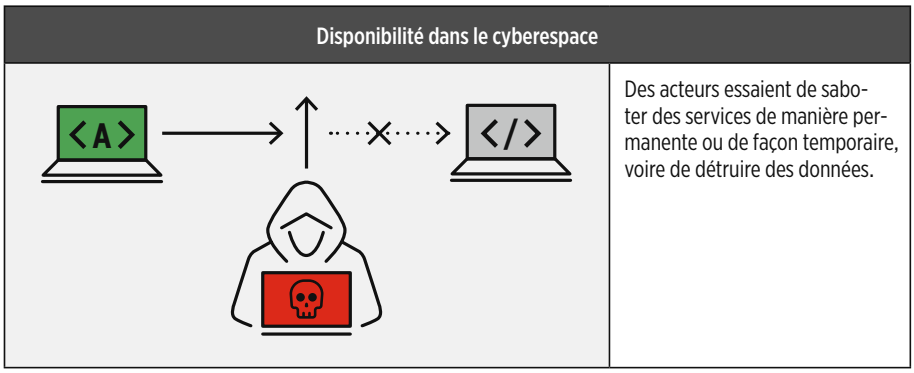


Illustration 10 : principe d'une attaque visant la disponibilité dans le cyberespace

La disponibilité des données peut être entravée par des cyberattaques, mais également par des actions dans l'espace électromagnétique, par exemple le brouillage radio. Ce procédé permet d'empêcher la réception d'informations transmises par ondes radio, de manière limitée dans le temps et l'espace. Les actions ne sont ainsi pas dirigées contre la disponibilité effective des informations dans les systèmes, mais contre la capacité technique à réceptionner des signaux.

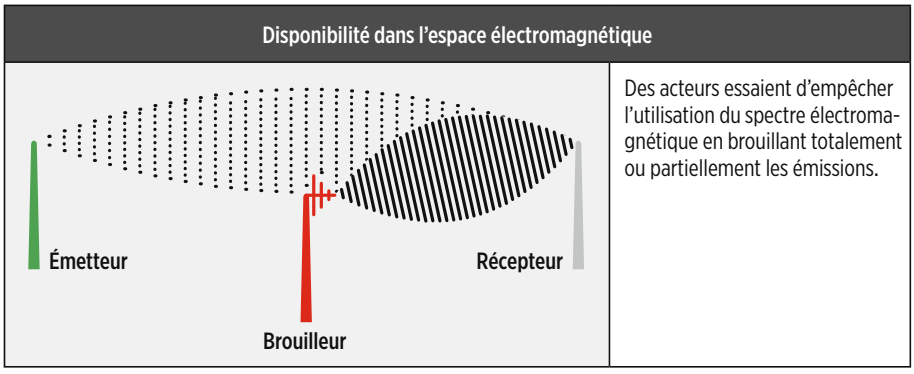


Illustration 11 : principe d'une attaque visant la disponibilité dans l'espace électromagnétique

4.3 Menaces

Les risques et les menaces dans le cyberespace sont multiples. Ils vont d'activités criminelles à l'engagement de cybermoyens offensifs dans un conflit armé en passant par des opérations d'espionnage, de manipulation et de désinformation. Afin de déstabiliser ou d'affaiblir les sociétés interconnectées, les assaillants utilisent toujours plus les possibilités découlant de la mise en réseau globalisée et de la numérisation. Un acteur peut au quotidien déjà agir sur le CYBEEM d'une partie adverse, sans pour autant devoir indubitablement s'identifier comme assaillant.

La situation en matière de menaces dans le CYBEEM est complexe. De nouvelles technologies sont développées en continu, au même titre que leurs applications techniques, ce qui crée en permanence de nouvelles interdépendances. Avec la numérisation, la vulnérabilité et le potentiel d'abus s'accroissent au sein du CYBEEM. Les actions dirigées contre les institutions étatiques et les infrastructures critiques peuvent massivement entraver le bon fonctionnement de l'administration, des forces armées et des autorités de sécurité. Elles peuvent dès lors avoir un impact direct sur la sécurité et l'ordre publics[94]. Les valeurs virtuelles telles que les cryptomonnaies, les lots de données, etc. gagnent en importance, ce qui augmente l'incitation à utiliser aussi le CYBEEM pour des activités criminelles. Les innovations technologiques et l'imbrication croissante des espaces physiques et virtuels débouchent sans cesse sur de nouvelles possibilités d'action[95].

Retracer le cours de cyberattaques est exigeant. Souvent, il est difficile de les attribuer à un seul acteur, ce qui peut conduire à des décisions erronées et augmenter le risque d'une escalade incontrôlée de la situation. Des acteurs peuvent dissimuler leur identité et leur intention ou même imputer leurs actions à des tiers non impliqués. Le vrai acteur agit sous couvert, faisant typiquement un usage ciblé de la désinformation. Divers ordres juridiques en partie non coopérants rendent par ailleurs plus difficile encore de poursuivre pénalement de telles actions et de les condamner[96]. Les frontières nationales ne jouent pratiquement aucun rôle dans le CYBEEM. À l'inverse, la souveraineté étatique et donc aussi l'ordre juridique sont principalement liés au territoire national. Comme l'infrastructure TIC se trouve le plus souvent sur le territoire d'un État[97], le CYBEEM ne se soustrait toutefois pas d'emblée à la souveraineté étatique. Les seules exceptions sont les infrastructures qui sont exploitées dans des régions qui ne sont attribuées à aucun État (p. ex. Mary-Byrd-Land en Antarctique).

Dans un contexte de menaces diffuses, il est essentiel d'analyser en permanence le potentiel de menace. À la différence des systèmes d'armes conventionnels, les cyberarmes ne peuvent être ni comptées ni directement comparées les unes aux autres. De plus, ce n'est plus tant exclusivement le matériel qui détermine la qualité des systèmes d'armes, mais de plus en plus les logiciels et la capacité à transformer les données brutes en informations utilisables.

---

94 Cf. Ministère fédéral allemand de l'intérieur : Une cyberstratégie en matière de sécurité pour l'Allemagne, 2016, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf [12.04.2020], p. 7.
95 Cf. Swisscom : Cyber Security Report 2019 : L'attaque ciblée, 2019, https://documents.swisscom.com/product/filestore/lib/c09ea7dd-a677-4d3a-883d-303240d36b8f/Swisscom_Security_Report_2019_FR.pdf [14.04.2020], p. 12.
96 Cf. Gaycken, Sandro/Talbot, David : Aufmarsch im Internet, in : Technology Review, 08.10.2010, https://m.heise.de/tr/artikel/Aufmarsch-im-Internet-1102301.html [12.04.2020].
97 Cf. Schulze, Sven-Hendrick : Cyber-»War» – Testfall der Staatenverantwortlichkeit, Tübingen, Deutschland : Mohr Siebeck, 2015, p. 113.

4.3.1 Acteurs

Acteurs étatiques

Dans la plupart des États, les effets dans le CYBEEM revêtent de l'importance avant tout pour les services de renseignement civils et les forces armées. De plus en plus de pays ont développé des approches leur permettant d'imposer leurs intérêts et intentions dans le CYBEEM aussi. Ce sont toujours avant tout les États qui édictent des lois et des régulations, définissent et imposent des normes techniques, régulent les marchés et s'assurent l'accès aux réseaux[98].

Services de renseignement

De nombreux services de renseignement déploient des cybermoyens pour rechercher des informations. Lorsque les objectifs en valent la peine, ils misent parfois sur des actions taillées sur mesure et ciblées (les menaces persistantes avancées, Advanced Persistent Threats), afin d'obtenir un accès durable aux ressources correspondantes. Le but peut être d'obtenir des avantages stratégiques, d'atteindre des buts politiques ou d'influer sur des évolutions technologiques à leur profit[99]. Pour les services de renseignement, il est déterminant d'agir le plus longtemps possible sans être repéré, afin d'espionner longuement (sur plusieurs mois) des informations sensibles ou de pouvoir causer d'autres dommages. Cela se fait en règle générale par une approche particulièrement prudente et difficile à retracer. De telles actions nécessitent beaucoup de ressources et présupposent des capacités techniques étendues[100].

En raison de l'interconnexion globale, les normes sont de plus en plus uniformisées. Cette uniformisation implique notamment que tous les acteurs ou presque utilisent le même matériel, produit en série, ce qui ouvre de nouvelles possibilités aux services de renseignement. Ils peuvent par exemple utiliser du matériel compromis (nuisible), équipé d'une porte arrière. Or la plupart du temps, un tel matériel est impossible à identifier ou presque. Il peut accéder à des données sans que les logiciels installés sur un système d'ordinateur le remarquent[101]. Il est possible d'introduire dans le matériel informatique utilisé dans le monde entier des vulnérabilités difficilement détectables, qui peuvent être facilement exploitées par des cyberattaques. Cela éveille des appétits chez les États d'obliger légalement les fabricants de matériel à collaborer, précisément aussi pour introduire de tels points faibles. Il est improbable qu'une entreprise privée s'oppose à son gouvernement dans ce contexte. Un service de renseignement peut également utiliser des portes arrière à des fins d'espionnage ou, en cas de crise, de sabotage. Les cybermenaces constituent ainsi un problème pour l'ensemble de la chaîne des fournisseurs[102].

Forces armées

Le CYBEEM est devenu aussi important pour les opérations militaires que les autres espaces d'opération. Les capacités CYBEEM constituent d'une part pour les forces armées un important multiplicateur de forces, en ce sens qu'elles peuvent renforcer les capacités militaires classiques. D'autre part, elles constituent une alternative d'action indépendante, pour compenser les propres faiblesses, raison pour laquelle des capacités additionnelles au combat électronique sont par exemple mises en place. En raison de la numérisation et de l'interconnexion croissantes, les frontières entre espaces d'opération se diluent toujours davantage[103]. Lorsque les forces armées disposent de capacités CYBEEM offensives, des options et alternatives d'action militaires addition-

---

98 Cf. Segal, Adam: The Hacked World Order, New York, United States: Public Affairs, 2016, p. 27.
99 Cf. Swisscom: Cyber Security Report 2019: L'attaque ciblée, 2019, https://documents.swisscom.com/product/filestore/lib/c09ea7dd-a677-4d3a-883d-303240d36b8f/Swisscom_Security_Report_2019_FR.pdf [14.04.2020], p. 17.
100 Cf. Ministère fédéral allemand de la défense: Abschlussbericht Aufbaustab Cyber- und Informationsraum, 2016, http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf [07.04.2020], p. 45.
101 Cf. Simonite, Tom: NSA's Own Hardware Backdoors May Still Be a « Problem from Hell », in: MIT Technology Review, 08.10.2013, https://www.technologyreview.com/2013/10/08/176195/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/ [04.05.2020].
102 Cf. Mäder, Lukas: Wenn der feindliche Zugang zum Computer gleich mitgeliefert wird, in: NZZ, 18.03.2019, https://www.nzz.ch/schweiz/wenn-der-feindliche-zugang-zum-computer-gleich-mitgeliefert-wird-ld.1467220 [03.05.2020].
103 Cf. Smeets, Max: The Strategic Promise of Offensive Cyber Operations, in: Strategic Studies Quarterly, vol. 12, 22.09.2018, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Smeets.pdf [03.05.2020], p. 90.

nelles s'ouvrent à elles. Elles peuvent manipuler, bloquer, perturber, dégrader et détruire des réseaux et des systèmes d'ordinateurs et d'information. Les actions menées dans le CYBEEM peuvent par ailleurs entraîner des effets qui ne sont pas possibles avec des actions conventionnelles.

Sur le plan international, on considère que les capacités CYBEEM offensives l'emportent sur les défensives[104], tant comme facteur de renforcement de la force de frappe que comme capacité autonome. **Il faut partir du principe que les grandes puissances et les puissances régionales allouent à leurs forces offensives des moyens financiers et en personnel six à dix fois supérieurs à ceux investis dans leurs forces défensives**[105]. Souvent, les cyber-actions constituent des alternatives présentant relativement peu de risques. Le seuil d'inhibition pour entraver des infrastructures TIC dans le cyberespace est ainsi plus faible qu'il ne l'est avec l'usage ouvert de la violence militaire dans le but d'atteindre des objectifs politiques ou militaires.

Les actions dans le CYBEEM peuvent également provoquer des dégâts dans l'espace physique, en particulier dans les infrastructures critiques. Si celles-ci sont perturbées, tombent en panne ou sont détruites, cela peut entraîner des conséquences graves sur la société, l'économie et l'État. Pour les forces armées, ce sont surtout les cyberattaques dirigées contre les infrastructures énergétiques qui sont problématiques, puisque celles-ci s'appuient souvent aussi sur une infrastructure civile pour approvisionner en énergie leurs systèmes militaires.

Les actions dans l'espace de l'information permettent aux forces armées de mener des opérations de déstabilisation et de subversion, et donc de saper ou de renverser l'ordre étatique établi. Elles visent à miner la confiance vis-à-vis des autorités, à perturber les relations, à discréditer les autorités et à affaiblir les structures étatiques. Le fait que des informations soient contrôlées ou manipulées pour des motifs politiques ou militaires n'a fondamentalement rien de nouveau en soi. La diffusion massive de technologies d'information et de communication a toutefois considérablement renforcé le mode opératoire. Grâce à des actions dans l'espace de l'information, il est possible de réduire l'engagement de moyens militaires conventionnels, voire d'éviter carrément une intervention armée ouverte[106].

Outre le cyberespace, l'espace électromagnétique revêt aussi une grande importance pour les forces armées. Les liaisons non câblées constituent ainsi l'épine dorsale des forces armées modernes. Seul celui qui contrôle l'espace électromagnétique peut engager avec succès des moyens militaires, car de plus en plus de systèmes d'exploration, de systèmes de conduite et d'effecteurs sont reliés les uns aux autres à travers l'espace électromagnétique. Le contrôle exercé sur l'espace électromagnétique constitue le prérequis nécessaire pour une conduite interconnectée des opérations en temps réel. Plusieurs pays émergents tels que la Russie ont dès lors massivement développé leurs capacités dans ce domaine au cours de ces dernières années. Il devient ainsi de plus en plus probable que des conflits aient lieu dans l'espace électromagnétique aussi[107].

Outre les moyens habituels du combat électronique, diverses forces armées ont développé de nouvelles armes à haute énergie ou à tout le moins leurs prototypes. Elles émettent un rayonnement électromagnétique et peuvent désactiver momentanément, perturber ou détruire intégralement des équipements, des installations ou du personnel se trouvant près d'elles. Peu de recherches ont été menées à ce jour pour savoir com-

---

104 Cf. Slayton, Rebecca : What Is the Cyber Offense-Defense Balance ? Conceptions, Causes and Assessment, in : International Security, Cambridge, United States ; The MIT Press, tome 41, 3e éd., 2017, p. 72–109.
105 Cf. Ruhmann, Ingo : Aufrüstung im Cyberspace. Staatliche Hacker und zivile IT-Sicherheit im Ungleichgewicht, in : Wissenschaft & Frieden, dossier 79, 3e éd., 2015, https://wissenschaft-und-frieden.de/seite.php?dossierID=083 [09.04.2020].
106 Cf. MacKenzie, Paul : Cyberspace and Cyber-Enabled Information Warfare, in : Joint Air Power Competence Centre, 2018, https://www.japcc.org/cyberspace-and-cyber-enabled-information-warfare/ [03.05.2020].
107 Cf. Schürz, Torben : Der vernetzte Krieg. Warum moderne Streitkräfte von elektronischer Kampfführung abhängen, in : DGAPkompakt 17, 16.10.2015, https://dgap.org/system/files/article_pdfs/2019-17-DGAPkompakt.pdf [08.04.2020].

ment de telles technologies impacteraient les systèmes actuels d'infrastructures (critiques) et quels effets en cascade générerait potentiellement leur engagement. Ce qui est sûr toutefois, c'est que de telles actions dans l'espace électromagnétique pourraient sévèrement toucher les sociétés et s'accompagner de conséquences sans précédent[108].

Contractants

Les contractants sont des entreprises privées proposant des prestations dans les domaines de la sécurité nationale, de l'armée et des services de renseignement. Il y a aussi à cet égard des prestataires qui remplacent ou complètent les capacités de mandants étatiques dans le cyberespace et l'espace de l'information. Ces organisations disposent de compétences que les États ne veulent pas détenir ou disposer en quantité insuffisante. Elles déploient leurs compétences soit dans le cadre d'une convention contractuelle avec l'État concerné, soit en agissant en toute autonomie, avec la tolérance expresse de l'État en question. Les contractants disposent des capacités, de l'organisation et de la détermination nécessaires pour mener eux-mêmes les actions les plus difficiles.

Grâce à ce jeu complexe avec des contractants, les États se ménagent un avantage, surtout ceux qui seraient inférieurs d'un point de vue strictement militaire ou qui ne veulent pas être reliés aux actions commanditées. En confiant à un contractant l'exécution d'actions clandestines dans le cyberespace et l'espace de l'information, un État peut se protéger d'une accusation ultérieure. Il peut ainsi poursuivre ses objectifs stratégiques et politiques en passant inaperçu, même si un autre État devait lui attribuer l'action en question. Le gouvernement accusé peut en effet simplement affirmer qu'il s'agit d'une activité criminelle, pour laquelle il n'est en rien responsable.

Différents États saluent la ratification d'un cadre juridique contraignant pour les actions dans le cyberespace et l'espace de l'information. Pour les États fonctionnant de manière subversive, cela reste en revanche un avantage de renvoyer vers des doutes juridiques réels ou uniquement allégués ou même de saper activement les efforts consentis pour fixer des normes de comportement contraignantes. Même si la communauté internationale réussissait à codifier et limiter de telles actions en accord avec le droit international, il subsisterait toujours une zone juridique grise avec l'engagement de contractants pour les actions CYBEEM[109].

Acteurs non étatiques

Les États restent certes dominants dans le contexte politique international, mais les acteurs non étatiques luttant également pour gagner en influence et en reconnaissance à l'échelle internationale deviennent aussi plus importants. Du fait des progrès technologiques et du développement des TIC modernes, les réseaux transnationaux non étatiques prennent de l'importance. Les logiciels potentiellement très nuisibles étant faciles à acquérir et peu coûteux, les États ne sont pas les seuls à disposer de moyens efficaces pour mener des actions dans le CYBEEM. Les groupes terroristes, les organisations criminelles et les individus expérimentés peuvent en effet eux aussi, avec peu de moyens, causer des dégâts potentiellement importants.

Font partie des acteurs non étatiques actifs dans le CYBEEM les cyberterroristes et les cyber-extrémistes, les cybercriminels, les hacktivistes et d'autres individus isolés.

Cyberterroristes et cyberextrémistes

S'agissant des terroristes et des extrémistes violents, il peut s'agir d'un groupe infraétatique, d'un réseau d'individus ou d'un individu isolé. Les terroristes et les extrémistes

---

108 Cf. Académie autrichienne des sciences : Digitaler Stillstand, Die Verletzlichkeit der digital vernetzten Gesellschaft, 2017, http://epub.oeaw.ac.at/0xc1aa5576_0x00358488.pdf [03.03.2020], p. 5–6.
109 Cf. Sigholm, Johan : Non-State Actors in Cyberspace Operations, in : Journal of Military Studies, vol. 4, 2013.

visent des objectifs différents avec leurs actions dans le CYBEEM, afin de diffuser leurs idéologies et d'élargir ainsi leur influence[110].

Il s'agit à cet égard de faire la distinction entre cyberterrorisme et terrorisme classique. Le cyberterrorisme travaille uniquement avec des TIC et n'opère que dans le CYBEEM. Le terrorisme classique recourt lui aux TIC pour planifier, appuyer et propager ses actions ou pour assurer la communication électronique entre les différentes cellules ou les membres du commandement.

Il y a parfois la crainte que des terroristes et des extrémistes violents exécutent des actions étendues dans le CYBEEM, notamment contre des infrastructures critiques. Une telle action ne constituerait pas seulement un grand succès en matière de propagande, mais entraînerait aussi des conséquences étendues sur l'économie nationale concernée. Aucun cas n'a toutefois été rendu public jusqu'ici où de tels groupes auraient poursuivi et atteint leurs objectifs stratégiques en menant uniquement des actions ciblées dans le CYBEEM. On n'a pas non plus encore identifié d'organisation terroriste qui soit capable de provoquer des dégâts physiques significatifs grâce à des actions ciblées dans le CYBEEM[111]. Les terroristes vont toutefois continuer à utiliser les TIC pour s'organiser, recruter du personnel, faire de la propagande, acquérir des fonds, collecter des informations, susciter des actions de sympathisants et coordonner des opérations[112]. Bien qu'il n'y ait pas eu de pur cyberterrorisme jusqu'ici, cette forme de menace ne peut pas être catégoriquement exclue.

Cybercriminels

Comme toute autre organisation utilisant des TIC, les forces armées peuvent devenir des cibles de la cybercriminalité, qui est devenue une affaire rentable et en pleine expansion. La gamme va de la petite délinquance simple à la cybercriminalité organisée avec un partage du travail élevé. La numérisation croissante, l'interconnexion omniprésente, la hausse exponentielle du nombre d'appareils interconnectés et le développement fulgurant de services basés sur des clouds créent de nombreuses vulnérabilités.

Le but des cybercriminels n'est pas en soi de compromettre le fonctionnement de la société, de l'État ou de l'économie. Ils sont toutefois prêts à causer d'importants dégâts collatéraux pour remplir leurs desseins criminels[113]. Pour autant que les actes de cybercriminalité soient découverts, ils restent pour la plupart impunis et ne sont même pas dénoncés. L'accès aux moyens de preuve électroniques est souvent difficile et des problèmes surviennent lorsque les cas sont portés devant les tribunaux. Les procédures complexes et les défis juridiques liés au caractère transfrontalier de la cybercriminalité font que les procédures tirent souvent en longueur[114]. De tels retards transforment ainsi quelques pays en zones de repli sûrs pour des cybercriminels[115].

Hacktivistes

Les hacktivistes utilisent les TIC comme moyens de protestation, afin d'atteindre des objectifs politiques ou idéologiques. Les actions typiques vont de la défiguration de sites Internet au dévoilement de documents confidentiels en passant par l'inondation des sites web de demandes diverses et variées. Des groupes plus importants lancent

---

110 Cf. Post Jerrold ; Ruby Keven ; Shaw Eric : From Car Bombs to Logic Bombs : The Growing Threat from Information Terrorism, in : Terrorism and Political Violence, vol. 12, 2e éd., London, United Kingdom : Taylor & Francis Group, 2000, p. 100.
111 Cf. Evan, Tamara : Cyber Terrorism Threat Intelligence and Loss Modelling, in : Cambridge Centre for Risk Studies 2018 Risk Summit, 2018, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/180620-slides-evan.pdf, [21.04.2020], p. 5.
112 Cf. Coats, Daniel : World Wide Threat Assessment of the US Intelligence Community, 13.02.2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf [21.04.2020], p. 6.
113 Cf. Unité de pilotage informatique de la Confédération (UPIC) : Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022, https://www.newsd.admin.ch/newsd/message/attachments/52072.pdf [29.04.2020], p. 3–4.
114 Cf. Parlement européen : proposition de résolution du Parlement européen sur la lutte contre la cybercriminalité, 25.07.2017, https://www.europarl.europa.eu/doceo/document/A-8-2017-0272_FR.html [27.04.2020], article M.
115 Cf. Microsoft : lutte moderne contre la cybercriminalité : recommandations d'action, https://news.microsoft.com/cloudforgood/_media/downloads/fr/modern-cybercrime-prevention-fr.pdf [27.04.2020], p. 1.

aussi des campagnes contre des organisations terroristes ou contre des États qui s'opposent à l'indépendance d'Internet.

Les hacktivistes ne visent en règle générale pas à tirer des avantages matériels ou financiers de leurs actions. Leur motivation tient de la volonté d'exercer de l'influence[116]. Les approches varient, en fonction des moyens à disposition, des capacités technologiques, de la cible et de la motivation. Les dégâts qui en découlent sont quant à eux acceptés ou même recherchés, pour attirer davantage l'attention. Souvent, des gouvernements, des organisations ou des branches entières sont visés par des actions de hacktivistes[117].

Autres individus isolés

Les autres individus isolés (p. ex. ceux appelés Script Kiddies ou Recreational Hackers) sont la plupart du temps des jeunes qui, en dépit de connaissances de fond lacunaires, tentent de pénétrer dans des systèmes ou réseaux de tiers ou de causer d'autres dommages. Leurs actions se caractérisent avant tout par la curiosité, par l'envie d'expérimenter et par le cybervandalisme. Ils choisissent leurs cibles de manière non spécifique. Il est également tout à fait possible qu'un système soit attaqué par le plus grand des hasards, même si cela dépend bien sûr du niveau de protection dudit système.

Les individus isolés utilisent des maliciels efficaces prêts à l'emploi ou des outils d'attaque automatisés, que l'on trouve très facilement sur Internet. Souvent, ils ne connaissent pas la pleine fonctionnalité de ces outils et ne comprennent pas le contexte technologique dans lequel ils s'inscrivent, ce qui ne les rend pas moins dangereux. L'une des plus grandes pannes de réseau de l'histoire a ainsi été causée par des individus imprudents en octobre 2016 sur la côte est des États-Unis. Ils ont transformé une multitude d'appareils ménagers connectés en un réseau d'attaque et ainsi provoqué une panne du web pour des millions de ménages américains (Distributed Denial of Service Attack, DDoS)[118]. Il faut enfin mentionner que quelques cyberattaques très exigeantes et pointues peuvent parfaitement être menées par des acteurs appartenant à cette catégorie. Un potentiel de menace à prendre au sérieux en résulte isolément.

	Acteurs étatiques			Acteurs non étatiques			
Espaces d'opération	Forces armées	Services de renseignement	Contractants	Cyberterroristes Cyberextrémistes	Cybercriminels	Hacktivistes	Individus
Cyberespace	●	●	●	◌	●	●	●
Espace de l'information	◐	●	●	◌	◐	●	●
Espace électromagnétique	●	●	◐	◌	◐	◐	◐

● S'est manifesté en priorité ◐ S'est manifesté en partie ◌ Ne s'est pas encore manifesté jusqu'ici – Non attendu

Illustration 12 : aperçu des acteurs et des espaces d'opération

116 Cf. Office fédéral allemand de la sécurité dans la technique d'information : Cyber-Bedrohungen – ein Einstieg, 09.08.2012, BSI - Bundesamt für Sicherheit in der Informationstechnik [17.04.2020], p. 2.
117 Cf. Gaycken, Sandro : Einführung Cyberwar : Was ist Cyberwar, 2013, https://www.inf.fu-berlin.de/groups/ag-si/pub/Cyberwar_SB1-5_V160114.pdf [28.04.2020], p. 18.
118 Cf. Gilbert, David : A bunch of kids probably pulled off the biggest DDoS hack ever, in : Vice News, 04.11.2016, https://www.vice.com/en_us/article/3k58e5/a-bunch-of-kids-probably-pulled-off-the-biggest-ddos-hack-ever [29.04.2020].

4.3.2 Autres risques

Outre les actions ciblées et intentionnelles, des inaptitudes humaines, des pannes techniques ou des catastrophes naturelles peuvent aussi entraîner des entraves dans le CYBEEM. Les événements de ce type ne peuvent en fin de compte pas être totalement évités. Ils surviennent régulièrement, sous des formes et des ordres de grandeur les plus divers. À l'origine de ces événements, on retrouve souvent non pas des actions ciblées, mais un enchaînement de circonstances malheureuses, couplé à des mesures de protection et de préparation insuffisantes. En raison de l'interconnexion de domaines les plus variés, la complexité a augmenté, ce qui fait qu'il est difficile d'estimer et de limiter les effets d'événements non intentionnels ou inévitables[119]. Malgré tout, il ne faut pas oublier que des circonstances et des incidents isolés apparemment malheureux pourraient aussi faire partie d'une action ciblée.

4.3.3 Infrastructure

Pour ce qui est des infrastructures critiques CYBEEM, il s'agit avant tout d'entreprises actives dans l'approvisionnement en énergie et la transmission de données, dans les chaînes (globales) d'approvisionnement en biens, mais aussi dans le domaine de la santé à l'échelle nationale et internationale. L'exemple de la transmission câblée mondiale de données permet de mieux appréhender le défi que cela représente en lien avec le CYBEEM, car de grandes parties du trafic international de données et de communications s'effectuent aujourd'hui via des câbles sous-marins. Si un seul d'entre eux venait à être endommagé, une région entière pourrait être coupée du CYBEEM sur une longue période. La conséquence en serait une entrave majeure des intérêts économiques et sécuritaires des États concernés[120].

4.3.4 Observations

L'État contribue à protéger la société et l'économie contre les menaces. À l'ère de la numérisation, il ne pourra s'acquitter de cette tâche que s'il peut offrir un certain degré de protection dans le CYBEEM également. Pour ce faire, il doit en premier lieu pouvoir protéger suffisamment ses propres systèmes. Le potentiel d'innovation numérique est énorme, aussi bien dans la perspective de nouvelles applications que de possibles menaces. Il est d'autant plus important que l'État recherche les développements possibles et de nouvelles solutions, sur la base d'une analyse des risques, et qu'il les intègre dans les concepts politiques[121]. En Suisse, on a développé à cet effet la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)[122]. L'armée y est intégrée dans le dispositif national global.

Les nouvelles menaces doivent être identifiées précocement, car une protection efficace exige des solutions innovantes. L'armée doit aussi contribuer à l'architecture nationale de sécurité CYBEEM. Cette contribution est décrite dans la SNPC. La Suisse ne pourra certes jamais ou presque suivre le rythme d'États agissant globalement pour ce qui est de la mise en place de capacités correspondantes, mais de nouvelles possibilités militaires pourraient toutefois naître pour l'Armée suisse aussi, avec les nouvelles marges de manœuvre dans le CYBEEM, en particulier sur le plan technique. À l'ère de la numérisation, la sécurité doit être considérée globalement. Afin que la sécurité puisse justement être garantie, les mesures nationales doivent être élargies tout en étant parallèlement imbriquées dans des processus régionaux et internationaux[123].

---

119 Cf. Unité de pilotage informatique de la Confédération (UPIC) : Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022, https://www.newsd.admin.ch/newsd/message/attachments/52072.pdf [29.04.2020], p. 5.
120 Cf. Patalong, Frank : Untersee-Kabel : Die fragilen Lebensadern des Internets, 02.02.2015, https://www.spiegel.de/netzwelt/web/untersee-kabel-die-fragilen-lebensadern-des-internets-a-1015809.html [29.04.2020].
121 Cf. Ministère fédéral allemand de l'intérieur : Cyber-Sicherheitsstrategie für Deutschland, 2016, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf [12.04.2020], p. 4.
122 Cf. Conseil fédéral : Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), 18.04.2018, https://www.newsd.admin.ch/newsd/message/attachments/52072.pdf [01.09.2020].
123 Cf. Kamasa, Julian : Pour une politique de sécurité transparente, 17.06.2019, https://www.avenir-suisse.ch/fr/de-la-necessite-dune-politique-de-securite-transparente/ [08.04.2020].

Le développement technique et organisationnel des menaces dans le CYBEEM représente un défi important et au long cours pour l'armée. Elle peut protéger sa propre capacité d'action en renforçant sa résilience et en prenant des mesures de sécurité à long terme et préventivement. Le développement de capacités CYBEEM est un prérequis pour ce faire. Celles-ci créent des options d'action additionnelles, afin d'éviter les conflits et gérer les crises[124]. Il est à cet égard essentiel que les moyens se développent de sorte que l'armée puisse s'acquitter de sa mission de protection et de défense à l'ère de la numérisation également et soit capable de se protéger efficacement contre des actions dans le CYBEEM.

L'armée se retrouve à cet égard au milieu d'un champ de tensions multidimensionnel. Elle doit aujourd'hui déjà relever les défis liés aux conflits et menaces actuels. Elle ne dispose toutefois pas encore de toutes les capacités effectivement nécessaires, malgré les progrès réalisés ces dernières années. Il s'agit donc de développer toute une série de nouvelles capacités permettant à l'armée de largement anticiper les menaces CYBEEM de tout type, de les combattre et de maîtriser rapidement et en continu les changements nécessaires. En première ligne, on retrouve ici la capacité de se protéger soi-même dans le CYBEEM, aussi contre les menaces futures. Il faut par ailleurs développer des capacités afin de pouvoir également agir activement dans le CYBEEM dans le cadre des missions de défense.

4.4 Supériorité en matière de savoir et de décision

4.4.1 Principes

Pour que les engagements de l'armée soient couronnés de succès, la rapidité avec laquelle les informations peuvent être rendues utilisables pour le commandement est déterminante. Celui des deux adversaires qui décide plus rapidement, par exemple où engager des formations ou des armes, garde la main. À l'échelle internationale, on parle dans ce contexte de la boucle OODA. Il s'agit d'un cycle de décision visant à pousser l'adversaire dans le rôle de celui qui doit réagir. Ceci s'obtient en exécutant le plus rapidement possibles les quatre étapes de la boucle, à savoir observer (Observe), apprécier (Orient), décider (Decide) et agir (Act).

Concrètement, il s'agit d'obtenir et de maintenir vis-à-vis d'un adversaire un avantage dans le temps en termes de savoir et de prise de décision, afin de pouvoir imposer ses propres buts avec des moyens limités. Une supériorité en termes de savoir s'obtient soit à l'aide de son propre avantage en la matière soit à travers le déficit en la matière de l'adversaire. Un avantage propre en termes de savoir s'obtient lorsque les données sont plus actuelles et mieux disponibles, lorsque leur véracité est garantie ou lorsqu'elles peuvent rapidement être évaluées. Un déficit adverse en termes de savoir s'obtient par exemple en camouflant ses propres moyens, en trompant l'adversaire avec des informations erronées ou encore en entravant ses systèmes de conduite à travers des cyberattaques.

124 Cf. Ministère fédéral allemand de la défense : Abschlussbericht Aufbaustab Cyber- und Informationsraum, 2016, http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf [07.04.2020], p. 1–2.

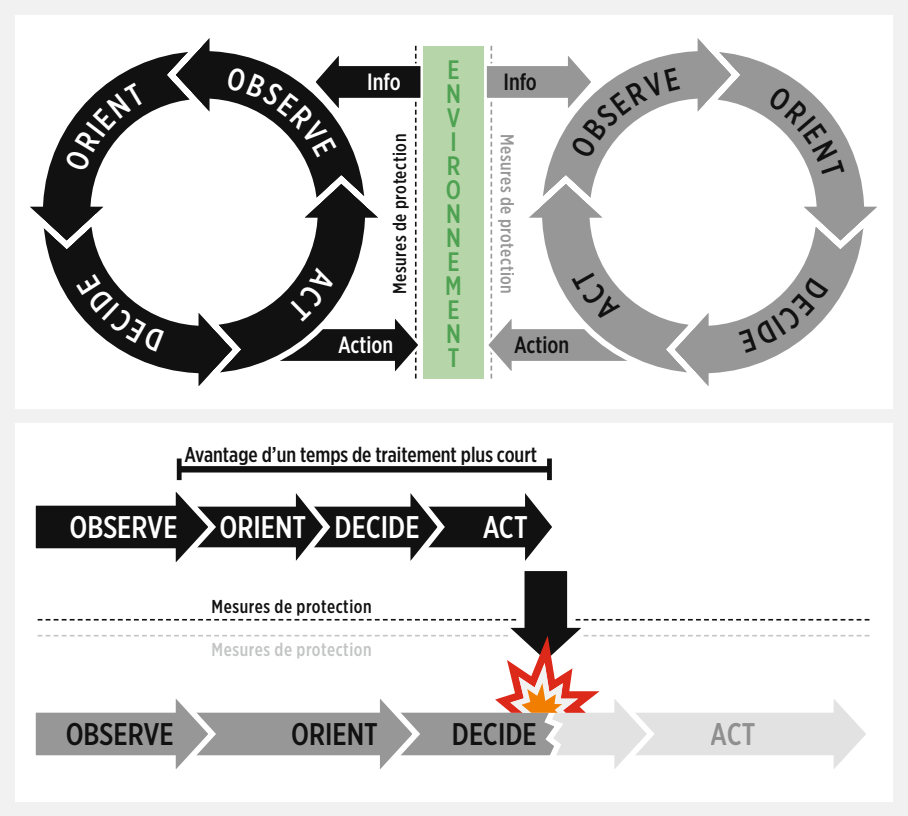


Illustration 13 : principe de la supériorité en matière de savoir et de décision

Outre l'avantage en termes de savoir, les forces armées visent aussi à obtenir une supériorité en matière de décision vis-à-vis de l'adversaire. Il s'agit à cet égard d'agir plus rapidement qu'un adversaire ou de le ralentir activement dans ses actions. On distingue ici deux approches, une défensive et une offensive.

Dans l'approche défensive, il s'agit de protéger à tout instant les systèmes propres, l'infrastructure technique et les propres informations contre les actions de l'adversaire. Cela peut se faire dans tous les espaces d'opération : les troupes GE peuvent par exemple protéger les transmissions radio entre systèmes, les cyberspécialistes peuvent garantir la protection des systèmes TIC alors que les troupes terrestres et les forces aériennes peuvent protéger des infrastructures (techniques) choisies contre les actions adverses. Le but est d'empêcher que l'adversaire puisse obtenir un avantage.

Une approche offensive vise quant à elle à provoquer un déficit chez l'adversaire en termes de savoir et de décision. Différentes troupes peuvent également être engagées à cet effet. Les cyberactions impactent la confidentialité, l'intégrité et la disponibilité des données dans les systèmes de traitement des informations de l'adversaire ; les actions dans l'espace électromagnétique servent à rechercher des renseignements et à perturber des signaux radio. Enfin, les attaques au sol ou dans les airs permettent de neutraliser d'importantes infrastructures adverses ou des parties de systèmes mobiles.

4.4.2 Quotidien

Au quotidien, l'armée doit avant tout se protéger contre des acteurs qui ont des intentions criminelles et relevant du renseignement. L'objectif est de garantir la disponibilité de l'armée. De plus, cette dernière s'acquitte au besoin dans le CYBEEM de missions subsidiaires et de tâches qui lui sont confiées par la loi.

Le cyberespace propre englobe les données, les informations et les systèmes TIC de l'armée. Il est relié au cyberespace global. Pour l'armée, l'autoprotection dans le cyberespace propre signifie identifier à tout moment les cyberattaques et empêcher les

assaillants d'atteindre leurs objectifs. Dans le cyberespace, l'armée recherche des informations sur l'étranger au profit des commandements politique et militaire, tout en devant à tout instant respecter les prescriptions légales. Dans le cadre de la cyberdéfense militaire, elle se tient par ailleurs prête à exécuter des actions propres contre des systèmes tiers, à chaque fois avec l'autorisation du Conseil fédéral.

Les systèmes TIC de l'armée peuvent être élargis à l'aide de systèmes radio, indépendamment de leurs emplacements. L'armée définit et administre à cet effet les fréquences dont elle a besoin pour la transmission des données. En collaboration avec les instances civiles, elle garantit la disponibilité des fréquences propres. Si les dispositions légales le permettent, l'armée et l'administration militaire recherchent des informations à l'étranger pour la conduite politique, militaire-stratégique et opérative et au profit du service de renseignement civil (SRC). L'armée assure par ailleurs la disponibilité au combat électronique.

Au quotidien, en cas de tensions et de conflits, l'armée surveille en permanence la situation militaire dans le CYBEEM. En complément et lors d'incidents, on assiste partout où la loi le prévoit à un échange permanent et à une coordination avec le SRC, responsable de la situation globale, ainsi qu'avec des partenaires. Les moyens techniques doivent être aptes à fournir au pied levé des prestations pendant plusieurs semaines ou mois.

Afin de pouvoir maîtriser les défis technologiques dans le CYBEEM et recruter les spécialistes requis, l'armée utilise le potentiel national en matière de formation, de recherche et d'économie. Pour ce faire, elle collabore avec des acteurs technologiques suisses (p. ex. des entreprises, start-ups ou hautes écoles) disposant de savoir-faire dans le CYBEEM. Enfin, elle utilise et encourage le savoir-faire présent au sein de la milice, et ce dès la formation militaire de base.

L'armée surveille l'évolution technologique dans le CYBEEM à quatre niveaux : évolutions futures, application pratique de nouvelles technologies, développement des technologies utilisées et réutilisation de technologies anciennes ayant fait leurs preuves[125]. L'accent est mis sur la déduction de mesures pratiques, afin de maintenir les capacités et de les étendre. Pour ce faire, l'armée travaille étroitement avec ses partenaires au sein de la Confédération, en particulier avec armasuisse.

4.4.3 Tensions

Il se peut que la situation dans le CYBEEM soit considérée comme tendue bien avant que la situation ne s'aggrave dans les autres espaces d'opération. Les acteurs qui utilisent des formes hybrides de conflit visent à passer inaperçus aussi longtemps que possible et à atteindre leurs objectifs sans faire usage ouvertement de la violence. Les cyberattaques et les actions dans l'espace électromagnétique constituent un moyen idéal à cet effet, car elles agissent à distance et ne sont que difficilement attribuables. Dans un contexte marqué par les conflits hybrides, l'armée doit avant tout affirmer son propre avantage en termes de savoir et de prise de décision. La protection propre revêt ici une importance centrale.

Il est probable que les cybermoyens de l'armée seraient en grande partie déjà utilisés dans une telle situation. Aux côtés des moyens de l'exploitation TIC de l'armée, ils assureraient la cyberdéfense militaire. Ceci se ferait de manière partiellement décentralisée, afin que l'armée puisse garantir la protection à l'aide de systèmes TIC partiels locaux en cas de panne partielle des TIC. Afin d'améliorer la protection propre, les systèmes TIC ne revêtant aucune importance pour l'engagement seraient par ailleurs découplés ou mis hors service.

125 Exemple pratique : pour l'enregistrement d'importantes quantités de données avec toute la sécurité, robustesse et durabilité requises (avant tout lors de backups), on utilise aujourd'hui à nouveau davantage des lecteurs de bandes magnétiques.

Les mesures propres, l'armée les coordonnerait en continu avec ses partenaires à l'échelon de la Confédération et dans le cadre du RNS. Avec ses cyberforces, l'armée pourrait par ailleurs fournir un appui subsidiaire. Dans le même temps, elle mènerait des actions pour identifier des réseaux tiers (virtuels) dans le cyberespace propre, y pénétrer et y rechercher des renseignements sur des acteurs adverses. Pour les actions menées contre des réseaux tiers hors du cyberespace propre, l'armée a besoin d'une autorisation du Conseil fédéral.

Dans l'espace électromagnétique, les voies d'attaque devraient être identifiées et si nécessaire fermées. Les fréquences propres seraient attribuées et surveillées et les brouillages éliminés. La disponibilité de l'armée et des systèmes serait augmentée en fonction de l'approche des acteurs adverses et de l'évolution possible de la situation. Il s'agirait par ailleurs d'identifier les brouillages radio visant les systèmes propres (p. ex. dans le secteur d'approche d'un aérodrome) et de lancer des mesures de protection et de défense appropriées. À l'intérieur du pays, l'armée se tiendrait prête à appuyer subsidiairement les autorités à l'aide de prestations dans l'espace électromagnétique, par exemple l'OFCOM pour ce qui est du monitorage des fréquences.

armasuisse appuierait davantage l'armée avec des expertises et des spécialistes. Elle acquerrait par ailleurs rapidement des moyens supplémentaires pour l'armée en cas de besoin, tels que des logiciels et du matériel ou des prestations spécialisées de l'industrie. Des spécialistes d'armasuisse pourraient être intégrés directement dans l'administration militaire et la soutenir sur place. Grâce à ses analyses, portant par exemple sur de nouveaux instruments d'attaque ou procédés électromagnétiques de transmission, elle soulagerait davantage encore l'administration militaire.

4.4.4 Conflits

En cas de conflit également, il s'agirait pour l'armée d'obtenir une supériorité en matière de savoir et de décision par rapport à des adversaires et de l'affirmer. Pour ce faire, elle devrait déployer des moyens issus de toutes ses composantes. Des infrastructures TIC de l'adversaire pourraient par exemple être détruites à l'aide de moyens adéquats, comme des attaques précises venant des airs ou des actions directes de forces spéciales. Il faudrait s'attendre à ce que les acteurs non impliqués directement utilisent la situation conflictuelle pour atteindre par exemple leurs objectifs criminels. Eux aussi pourraient continuer à exercer de la pression dans le CYBEEM sur l'armée ou la renforcer. L'armée suspendrait par conséquent l'exploitation de tous les systèmes TIC qui ne sont pas importants pour l'engagement, afin de mieux se protéger.

Les cyberforces devraient par ailleurs fournir des prestations décentralisées offensives pour appuyer le combat. Dans ce contexte, l'accent serait mis sur les actions CYBEEM combinées visant les systèmes de l'adversaire. Des renseignements pourraient en outre être recherchés à l'aide de la forensique dans le secteur d'engagement. Les appareils TIC trouvés ou volés (p. ex. smartphones ou vecteurs de données) seraient pour ce faire analysés sur place.

En cas de conflit, les effets nécessaires dans l'espace électromagnétique seraient garantis en permanence grâce à l'engagement combiné de toutes les forces GE. La capacité de l'exploration propre revêt à cet égard une importance particulière. Il s'agirait de la protéger contre les effets des armes de longue portée. Par ailleurs, des emplacements de rechange seraient mis à disposition et au besoin déployés pour les centrales d'engagement, de même que des solutions de remplacement pour les capteurs détruits.

5

Capacités

Les capacités dans l'espace électromagnétique et le cyberespace ne remplacent pas celles au sol ou dans les airs. Elles les renforcent et les complètent, les rendant plus efficaces, mais aussi plus dangereuses.

Fondamentalement, l'Armée suisse dispose aujourd'hui déjà de toutes les capacités CYBEEM nécessaires pour l'avenir, mais pas toujours au niveau requis.

5 Capacités

Le présent chapitre décrit les capacités dont l'armée doit disposer dans le CYBEEM à l'horizon 2030 et au-delà pour pouvoir s'acquitter de sa mission à long terme et indépendamment de la situation. Ces capacités découlent des tendances concernant le contexte et les développements figurant au chapitre 2 et des réflexions doctrinales tirées du chapitre 4.

5.1 Exigences fondamentales en matière de capacités

Pour obtenir la supériorité nécessaire en matière de savoir et de décision, il faut pouvoir s'appuyer techniquement sur des TIC modernes, sûres et robustes. Celles-ci créent en outre les conditions préalables nécessaires à un réseau intégré de conduite numérisée. L'armée doit protéger en permanence cette fondation de la capacité de conduite. Elle suit ainsi aussi une exigence importante de la SNPC et du rapport 2021 sur la politique de sécurité, à savoir que tous les acteurs sont responsables de leur propre protection et doivent dès lors être en mesure de se protéger contre les risques et les menaces dans le cyberespace de la manière la plus autonome possible. Afin de pouvoir combattre un adversaire dans le CYBEEM et y rechercher des renseignements, l'armée doit pouvoir planifier et exécuter des actions militaires en toute autonomie. Il doit à cet égard être techniquement possible d'intégrer aussi des partenaires de manière flexible. Le commandement des Opérations veille à la coordination des effets à travers tous les espaces (Multi-Domaine). À l'avenir, l'armée devra par ailleurs pouvoir davantage mettre ses capacités à la disposition de partenaires au sein du RNS, d'autres services fédéraux et autorités, de partenaires économiques et de la société ou de tiers également, par exemple d'exploitants d'objets faisant partie de l'infrastructure critique. Le soutien est toujours apporté sur demande et n'intervient que les moyens des autorités civiles ne sont pas disponibles et ne peuvent pas non plus être fournis dans la quantité souhaitée et en temps opportun par des prestataires commerciaux (principe de subsidiaire).

Les tâches mentionnées doivent s'inscrire dans un cadre global formé par :

— le cadre juridique et les décisions politiques[126] ;
— le réseau de coopération en Suisse et à l'étranger pour l'échange d'informations ;
— le réseau des compétences disponibles en Suisse[127].

5.2 Détermination des capacités

Trois capacités autonomes découlent des exigences fondamentales en matière de capacités, à savoir l'autoprotection CYBEEM, les actions dans le cyberespace et les actions dans l'espace électromagnétique. L'autoprotection CYBEEM englobe tous les préparatifs techniques, opérationnels, organisationnels et tactiques pour se protéger des menaces. Font partie des actions dans le cyberespace et dans l'espace électromagnétique des mesures à la fois passives et actives. Les mesures passives sont par exemple l'exploration radio ; les actives l'intrusion dans un ordinateur tiers ou le brouillage radio.

Trois domaines permettent d'obtenir un avantage propre en termes de savoir et de prise de décision. Premièrement, l'armée a besoin de moyens pour transporter et traiter des données, ce qui est assuré par l'infrastructure TIC. Deuxièmement, il faut des

126 Décisions du Conseil fédéral, ordres, directives, interventions parlementaires, recommandations des organes de surveillance, stratégies et charges issues du rapport sur la politique de sécurité, Stratégie nationale de protection de la Suisse contre les cyberrisques et Stratégie nationale pour la protection des infrastructures critiques, Plan d'action Cyberdéfense DDPS
127 En première ligne dans la base technologique et industrielle, dans les universités et les hautes écoles, en collaboration étroite avec la division Sciences et technologies d'armasuisse.

mesures techniques et organisationnelles pour assurer le commandement de manière coordonnée à tous les échelons et avec tous les partenaires. Troisièmement, on a besoin de mesures et d'outils permettant de tirer des enseignements à partir de données et d'informations, afin d'obtenir une compréhension commune de la situation (p. ex. applications logicielles, moyens techniques, méthodes d'analyse des données et des informations, etc.).

Il en découle trois autres capacités dans le CYBEEM, qui sont aussi qualifiées de capacités de soutien de la numérisation, à savoir :

— une compréhension commune de la situation ;
— un traitement robuste et sûr des données ;
— une conduite conjointe sur le plan organisationnel et technique.

Le tableau ci-après inventorie toutes les capacités CYBEEM, avec un bref descriptif. Il garantit leur lien avec les champs d'action de la Stratégie cyber du DDPS.

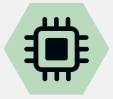
	**Autoprotection CYBEEM** Protéger les formations de troupe, les systèmes, les infrastructures, les informations et les réseaux au sein du CYBEEM contre des actions adverses. Concerne les champs d'action ci-après de la Stratégie cyber du DDPS : 2, 3, 5, 7b, 8, 9, 10, 12, 15.
	**Capacités opérationnelles de la numérisation**
	**Compréhension conjointe de la situation** Identifier les risques et les menaces, comprendre le contexte et identifier les chances et les évaluer de manière cohérente en réseau. Concerne les champs d'action ci-après de la Stratégie cyber du DDPS : 3, 5, 7b, 8a, 8b, 9, 16, 18.
	**Traitement robuste et sûr des données** Assurer le traitement et la diffusion des données en fonction de la mission et de la situation. Concerne les champs d'action ci-après de la Stratégie cyber du DDPS : 2, 3, 4, 5, 7b, 8a, 8b, 16.
	**Conduite en réseau – mesures organisationnelles et techniques** Assurer la conduite en réseau sur les plans tant organisationnel que technique en coordination avec les partenaires. Concerne les champs d'action ci-après de la Stratégie cyber du DDPS : , 4, 5, 7a, 8a, 8b, 18
	**Actions dans l'espace électromagnétique** Mener des actions dans l'espace électromagnétique. Concerne les champs d'action ci-après de la Stratégie cyber du DDPS : 2, 16.
	**Actions dans le cyberespace** Mener des actions dans le cyberespace. Betrifft folgende Handlungsfelder der Strategie Cyber VBS : 8a, 8b, 12, 14, 15, 18.

Tableau 1 : les capacités CYBEEM et leur imbrication dans la Stratégie cyber du DDPS

5.3 Capacité Autoprotection CYBEEM

5.3.1 Description

L'autoprotection CYBEEM englobe toutes les capacités qu'il faut pour protéger les formations, systèmes, infrastructures, données, informations et réseaux propres de l'armée contre les menaces dans le CYBEEM dans toutes les situations. Il peut s'agir d'actions adverses, de défaillances techniques ou humaines ou d'influences environnementales.

La gestion intégrale de la sécurité fait partie de l'autoprotection CYBEEM. Elle englobe des mesures techniques, organisationnelles et d'exploitation pour protéger les TIC. La gestion dite des points faibles TIC constitue un élément important dans ce contexte. Elle sert à identifier les éventuelles vulnérabilités et à les combler à titre préventif. Afin que les menaces puissent être anticipées, il faut de plus ce que l'on appelle un *Cyber Threat Intelligence & Technological Foresight*. La disponibilité à appuyer des partenaires ou des tiers dans le cadre de la subsidiarité fait également partie de l'autoprotection CYBEEM.

L'identification et la neutralisation des attaques visant les TIC de l'armée constituent une autre partie importante de l'autoprotection. Si l'attaque est neutralisée, les dommages provoqués doivent être constatés et les méthodes de l'assaillant analysées. D'autres informations sont par ailleurs recherchées, par exemple sur les outils logiciels utilisés, les intentions et les cibles des attaques. Les systèmes TIC retournent ensuite à leur état normal et les failles de sécurité utilisées par l'assaillant sont durablement comblées.

De nombreux capteurs et systèmes d'armes de l'armée utilisent l'espace électromagnétique. La liberté de manœuvre dans cet espace est donc décisive pour la conduite et l'engagement d'armes dans d'autres espaces d'opération (en particulier au sol et dans les airs). D'où l'importance centrale de l'autoprotection. Celle-ci consiste avant tout à saisir les activités électromagnétiques adverses, à alerter ses propres troupes et à prendre des contre-mesures, pour autant que cela soit nécessaire.

Dans l'espace électromagnétique, il s'agit par ailleurs de contrôler les émissions propres, soit l'image de ses propres émissions électromagnétiques. Cela permet de se soustraire à l'exploration radio adverse ou de l'induire en erreur. Il s'agit en outre d'empêcher que des capteurs et effecteurs propres se gênent mutuellement. L'image des propres émissions électromagnétiques est formatée à l'aide de mesures tactiques, organisationnelles, techniques ou opérationnelles.

5.3.2 Aspect futur

À l'avenir, l'armée devra conduire l'autoprotection CYBEEM de manière centralisée et l'assurer intégralement à travers tous les secteurs partiels du CYBEEM. Les deux formes décrites ci-après constituent la condition préalable nécessaire : l'autoprotection CYBEEM intégrale et l'anticipation des menaces et des risques.

Autoprotection CYBEEM intégrale

Aujourd'hui, il est difficile d'assurer l'autoprotection CYBEEM pour deux raisons principales : d'une part, parce que l'armée dispose de très nombreux systèmes différents et, d'autre part, parce que l'armée exploite des systèmes TIC qui ne sont pas reliés en permanence au réseau global. Il existe par ailleurs de nombreux systèmes isolés, en particulier pour les systèmes d'armes. L'armée doit dès lors acquérir la capacité de protéger à l'avenir l'ensemble de ses systèmes.

À l'heure actuelle, l'armée met l'accent principalement sur la protection centralisée des systèmes TIC et des réseaux qui sont reliés en permanence au réseau global. La centrale des opérations de l'autoprotection CYBEEM utilisée à cet effet devra à l'avenir être complétée par des sites de remplacement. Actuellement, il n'est par ailleurs pas possible ou presque d'assurer une protection décentralisée des systèmes et des infrastructures importantes, comme un centre logistique de l'armée. Il s'agit à cet égard de veiller à ce que l'armée acquière la capacité d'assurer une protection efficace sur place (de manière décentralisée).

Il est possible que l'armée soit exposée simultanément à plusieurs attaques dans le CYBEEM. Afin de pouvoir les neutraliser, il faut étendre la surveillance des systèmes et améliorer la capacité de résistance du personnel. S'agissant de la surveillance, il s'agit

avant tout d'identifier et de suivre les événements revêtant une importance sur le plan de l'autoprotection dans le CYBEEM, à l'échelle de l'armée et en permanence. Il faut par ailleurs établir des processus pour l'ensemble de l'armée qui permettent de maîtriser également des attaques contre des systèmes d'armes isolés.

La chaîne d'approvisionnement (supply chain) pour les systèmes TIC de l'armée n'est, elle non plus, pas encore intégralement assurée. Afin de combler cette lacune sur le plan des capacités, les composantes doivent pouvoir être contrôlées à travers toutes les interfaces accessibles. Cela vaut tant pour les logiciels que le matériel.

Avec le cryptage aujourd'hui habituel des canaux de communication, l'espionnage revêt à nouveau une importance accrue là où les informations ne sont pas encore cryptées, par exemple dans les salles de réunions ou les salles de commandement. Pour rechercher des informations, on utilise par exemple des puces ou des microcaméras cachées. Nos capacités de « lutte contre les écoutes » pour trouver de tels appareils sont actuellement très limitées et doivent être développées, avant tout sur le plan du personnel.

L'autoprotection CYBEEM s'étend aussi dans l'espace électromagnétique. Il faut à cet égard particulièrement tenir compte du fait que les acteurs les plus divers explorent en permanence l'espace électromagnétique, et ceci au quotidien déjà. Afin de se protéger contre une telle menace, il est essentiel de contrôler l'image de ses propres émissions. Cette capacité n'est aujourd'hui quasiment pas établie et doit être développée. Il faut pour ce faire développer et former les processus de planification et de conduite nécessaires.

Anticipation des menaces et des risques

L'armée devra à l'avenir mieux anticiper les menaces et les risques dans le CYBEEM, en utilisant encore plus rapidement et activement ses propres données collectées et les contributions de partenaires. Elle doit pour ce faire être en mesure de trouver des données à l'intérieur des propres systèmes (militaires) et de les interpréter à l'aide de méthodes modernes, ce qui lui permet d'ordonner en temps opportun des mesures de protection préventives.

Il est prévisible que des troupes aient un contact avec des traces numériques d'un adversaire lors d'un engagement, par exemple lorsqu'elles trouvent des supports de données. Ceux-ci peuvent contenir des informations décisives et doivent être analysés le plus rapidement possible. Ceci se fait au mieux directement sur le terrain, sans délai et de manière automatisée. La capacité de la « forensique dans le secteur d'engagement » n'existe pas actuellement et doit être développée.

5.4 Capacité Compréhension commune de la situation

5.4.1 Description

La compréhension commune de la situation permet de comprendre le contexte d'un engagement à tous les échelons de la conduite. Il faut à cet égard identifier les risques, dangers et menaces et mettre à profit les chances. Afin de gérer la quantité croissante de données, il faut s'appuyer sur l'automatisation, la numérisation et l'application de la science des données. Ces techniques permettent d'analyser plus rapidement des contextes complexes de manière détaillée. L'objectif est d'établir une image militaire d'ensemble de la situation et, en parallèle, des images spécifiques de la situation, axées sur les besoins. Il faut pour ce faire trouver, transmettre et traiter des données et des informations tout en automatisant la préparation et la présentation des informations.

5.4.2 Aspect futur

Une image fusionnée et actuelle de la situation est un prérequis déterminant pour le succès à l'engagement. Afin d'atteindre ce but, la représentation de la situation doit simplement pouvoir s'adapter aux besoins liés à l'engagement en question. Les données et les informations sont préparées à l'aide de la science des données avant d'être représentées sous la forme d'images de la situation de manière automatisée, en fonction des échelons et de la planification. Les conditions préalables nécessaires à cet effet sont une architecture uniforme en matière de données et d'informations, des TIC modernes et du personnel spécialisé ad hoc. Afin de pouvoir le garantir dans toutes les situations, la science des données a besoin de systèmes TIC particuliers *(High Performance Computing [HPM] Cluster)*.

Au cours de ces dernières années, de premières capacités en matière de science des données ont été développées au sein de l'armée dans quelques domaines spécialisés, par exemple l'exploration radio. Ces capacités ne sont toutefois conçues que pour un champ d'application spécifique et ne peuvent donc pas être utilisées pour d'autres. En raison du grand nombre de systèmes TIC différents et de la variété actuelle des formats de données, les données ne sont que difficilement interchangeables et ne peuvent pas être utilisées à l'aide de la science des données. Il existe dès lors dans ce secteur une importante lacune capacitaire. Afin de la combler, il faut notamment élaborer une stratégie en matière de données applicable à tous les domaines de l'armée. Celle-ci doit permettre d'introduire des formats de données uniformes dans l'ensemble de l'armée. Il faut de plus acquérir les systèmes TIC nécessaires et embaucher le personnel spécialisé requis. Étant donné que les coûts sont élevés et que les spécialistes requis ne sont disponibles que de manière limitée, la capacité de la science des données ne pourra se développer que dans des domaines choisis de l'armée. Ceux-ci doivent ensuite mettre leurs prestations à disposition des différents consommateurs. Seuls, les systèmes ne suffisent cependant pas. Ce qu'il faut, c'est aussi un changement de culture, de sorte que les données issues de divers domaines de l'armée puissent être échangées et utilisées en commun.

À l'exception des Forces aériennes, l'armée n'utilise encore que trop peu les nouvelles techniques déjà éprouvées en matière de représentation de la situation. En règle générale, les situations militaires complexes sont représentées en deux dimensions sur des écrans ou des moyens similaires. Cela complique la tâche consistant à saisir rapidement les situations ou à piloter simplement les systèmes. Les responsables doivent toutefois pouvoir interagir intuitivement, rapidement et simplement avec ces systèmes. Pour ce faire, on va à l'avenir aussi avoir davantage recours à des technologies telles que la réalité augmentée et virtuelle, afin d'améliorer les interfaces entre l'humain et les systèmes. Cette lacune doit être comblée dans les projets d'armement, par exemple lors de l'acquisition d'un nouveau système de conduite.

5.5 Capacité Traitement sûr et robuste des données

5.5.1 Description

La capacité d'assurer un traitement et une diffusion sûrs et robustes des données nécessite une infrastructure TIC qui soit intégralement protégée et extensible. Ceci est l'un des prérequis techniques en vue de la numérisation de l'armée. L'infrastructure TIC nécessaire à cet effet doit être aménagée de telle manière à ce qu'elle continue à fonctionner en cas d'interruptions du réseau ou de panne de l'alimentation électrique.

Ce qui est essentiel, c'est que la confidentialité, l'intégrité et la disponibilité des données soient garanties en permanence. Cela exige de vérifier régulièrement les mesures de protection et de les adapter. Les services d'identification et d'authentification veillent à ce qu'il soit techniquement possible d'accéder aux données en toute sécurité.

Les systèmes TIC utilisés par des partenaires aux exigences particulières sont gérés de manière hautement sécurisée dans des environnements isolés. En font par exemple partie ceux des services de renseignement.

5.5.2 Aspect futur

Le programme FITANIA en cours et l'architecture TIC 4.0 constituent une condition préalable nécessaire à la numérisation et ainsi au réseau numérique intégré de conduite qui est visé. Trois composantes forment le programme FITANIA : le réseau de transmission indépendant, les centres de calcul et le réseau de communication mobile de la troupe. L'architecture TIC 4.0 définit les principes supérieurs à long terme et les normes TIC applicables au sein de l'armée et dans la collaboration avec des partenaires.

Le réseau de transmission indépendant (Réseau de conduite suisse) est un réseau de transport de données stationnaire. Il fonctionne sur la base de câbles à fibres optiques et de liaisons par faisceau hertzien. Afin de maintenir sa disponibilité à un niveau élevé, différentes liaisons sont aménagées de manière redondante. Le réseau étendu doit permettre de transporter des données de manière cryptée entre chaque emplacement.

Trois nouveaux centres de calcul sont construits, permettant d'adapter l'infrastructure existante aux exigences futures de l'armée. Deux de ces centres seront mieux protégés, grâce à des mesures de sécurité accrues. Quant au troisième, qui se trouve dans une catégorie de protection moins élevée, les organes fédéraux civils pourront également l'utiliser.

Afin de transporter des données via le réseau de communication mobile de la troupe, il faut une mise en réseau protégée. Le traitement central des données est à cet égard complété par des moyens TIC autonomes et partiellement mobiles, par exemple avec des petits centres de calcul transportables. La troupe peut engager ces systèmes de manière flexible dans le secteur d'engagement. Le flux des données est garanti par une liaison à large bande à tous les échelons de commandement. Après la mise en œuvre de FITANIA, une importante lacune capacitaire subsistera, à savoir les *Business Support Services* (p. ex. courriels, applications spécialisées, etc.) pour les troupes et états-majors de la milice sur les lieux de l'engagement. Les projets d'acquisition nécessaires sont en phase d'initialisation.

Les *smart devices* (smartphones et appareils semblables) sont largement répandus dans la société. Cela offre la chance de mettre les services TIC de l'armée à disposition de nombreux militaires à moindres frais, par exemple via des applications. Si la situation le permet, les réseaux de télécommunication civils et militaires devraient à l'avenir pouvoir être utilisés de manière combinée pour la transmission des données. L'armée aura ainsi plus de flexibilité dans la transmission militaire des données. Dans le même temps, les moyens civils peuvent évidemment aussi s'accompagner de nouvelles exigences en matière de sécurité, dont il faut tenir compte déjà dans la conception de telles solutions.

5.6 Capacité Conduite conjointe sur le plan organisationnel et technique

5.6.1 Description

Cette capacité à la conduite conjointe garantit que les différents échelons de conduite et les partenaires disposent des informations opérationnelles nécessaires en fonction de la situation, en temps opportun et avec le bon degré de détail. Il faut pour ce faire des mesures organisationnelles et des interfaces techniques. Différents états-majors doivent par exemple collaborer sur le plan du contenu de manière coordonnée dans le temps et les systèmes de partenaires doivent pouvoir échanger des données. La ca-

pacité de la conduite conjointe permet de coordonner les activités de conduite et de concerter la démarche à travers tous les échelons de conduite et avec les partenaires.

Un échange harmonieux d'informations et de situations est incontournable à cet égard. Il s'effectue à différents niveaux, avec différents partenaires et est flexible dans le temps. La capacité de partager les informations nécessaires de manière si possible automatisée est élémentaire pour l'exécution de la mission et la coordination.

5.6.2 Aspect futur

La numérisation entraîne une forte hausse du flux de données. Dans un réseau numérique intégré de conduite, ces données doivent être partagées ou transmises d'un système à l'autre. Les flux de données très variables qui en découlent exigeront à l'avenir une gestion efficace des informations et des données. À cet égard, il s'agit d'assurer les flux de données entre toutes les personnes autorisées, à travers l'ensemble des organisations, échelons de conduite et systèmes.

L'armée dispose aujourd'hui de systèmes d'information pour la conduite qui sont en règle générale des systèmes dits en silo. La circulation des informations ne se fait pas en flux continus. Des interruptions de flux rendent l'échange d'informations compliqué et chronophage et favorisent les erreurs. Les données sont en partie transmises d'un système à l'autre à la main, ce qui est également problématique sous l'angle de la sécurité. Pour l'armée, il s'agit de mettre hors service les systèmes en silo existants et de les remplacer par de nouvelles solutions modernes. Celles-ci doivent permettre de mettre en place un réseau numérique intégré de conduite. Pour ce faire, il faut créer les conditions préalables et les bases légales requises et former les responsables requis dans les organisations concernées.

5.7 Capacité Actions dans l'espace électromagnétique

5.7.1 Description

Les actions dans l'espace électromagnétique servent à perturber la transmission radio adverse ou carrément à empêcher l'adversaire d'utiliser l'espace. Le but finalement est d'entraver l'adversaire dans sa quête visant à obtenir un avantage en termes de savoir et de prise de décision. La capacité en question englobe des mesures actives et passives. Les mesures actives sont par exemple le brouillage des communications radio, la localisation et le guidage; les mesures passives sont par exemple l'exploration radio, les alertes radar ou les contributions à la représentation de la situation aérienne. En font par ailleurs partie toutes les activités qui sont nécessaires pour garantir la disponibilité opérationnelle et augmenter la liberté d'action propre au quotidien déjà, en analysant par exemple des signaux électromagnétiques inconnus.

5.7.2 Aspect futur

Avec des actions dans l'espace électromagnétique, l'armée peut agir sur les capacités techniques de la conduite d'un adversaire, sans causer de dommages physiques ou carrément des destructions et sans mettre des vies humaines en danger. Cela donne notamment la possibilité à la troupe d'entraver l'adversaire dans sa conduite, pendant qu'elle mène des actions contre lui au sol. Les moyens permettant de mener des actions dans l'espace électromagnétique complètent, appuient et renforcent ainsi nettement la prestation au combat d'une unité de combat. Étant donné que ces moyens agissent à distance, la propre troupe est exposée à un risque bien plus faible qu'avec l'usage d'armes conventionnelles. Grâce à ces moyens de conduite des actions dans l'espace électromagnétique, la troupe se retrouve également en mesure d'empêcher l'adversaire de déclencher par radio des charges explosives, grâce par exemple au brouillage radio. Elle dispose ainsi d'un autre moyen pour assurer sa propre protection dans le secteur d'engagement. Globalement, la troupe obtient à travers ces moyens des pos-

sibilités supplémentaires pour exécuter des actions conformes au droit international et proportionnées, que ce soit au quotidien, en cas de tensions ou en situation de conflit. Ceci est d'autant plus important que les engagements militaires interviennent de plus en plus souvent dans des environnements densément peuplés.

La capacité de mener des actions dans l'espace électromagnétique est aujourd'hui en premier lieu axée sur la lutte contre une attaque armée. L'armée est actuellement en mesure d'explorer, de brouiller et d'entraver des systèmes radio tactiques. Elle dispose à cet effet de différents systèmes majeurs, originellement conçus dans la perspective d'une conception conventionnelle des conflits. Ces systèmes sont aménagés de telle manière qu'ils ne se prêtent pas bien aux engagements en terrain bâti et dans un contexte de conflit hybride. Les capteurs stationnaires existants seraient vraisemblablement détruits rapidement en cas de conflit, car leurs emplacements seraient sans doute connus. Ils sont ainsi une cible facile pour les armes à distance.

L'armée ne doit pas seulement axer ses futurs moyens sur la lutte centralisée contre des forces militaires agissant de manière conventionnelle, mais également sur des engagements contre de nouveaux types de cibles dans un contexte de conflit hybride. En complément aux systèmes majeurs, qui seront toujours nécessaires à l'avenir, des systèmes légers et faciles à engager sont nécessaires pour les troupes terrestres. Étant donné que de nouvelles contre-mesures sont développées en permanence à l'échelle internationale, l'armée doit pouvoir de plus rapidement adapter ses capacités à mener des actions dans l'espace électromagnétique. Il faut par ailleurs acquérir également des moyens pour la conduite de la guerre électronique qui soient capables d'agir dans le champ de fréquences des radars. Les infrastructures-clés de l'exploration radio, comme l'infrastructure de l'analyse centrale, doivent par ailleurs être aménagées de manière redondante.

L'armée doit à l'avenir disposer également de radars passifs. Il s'agit de radars capables d'identifier des objets sans pour autant émettre de signaux propres. Les systèmes actuels de radars émettent de forts signaux électromagnétiques. Ils peuvent ainsi être facilement localisés et détruits à l'aide d'armes à distance. Un radar passif utilise avant tout les signaux radio existants qu'il ne produit pas lui-même (p. ex. FM, DAB, DVB-T). Il est dès lors quasiment impossible de localiser un radar passif pour ensuite le détruire. Outre le radar passif, il faut aussi examiner plus à fond la technologie du radar dit bistatique. Il s'agit là d'un système de radar qui s'appuie sur une séparation géographique entre émetteur et récepteur.

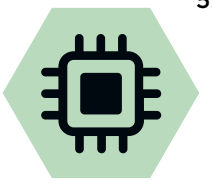
Une autre lacune capacitaire ressort à l'exploration des systèmes radio à ondes courtes. De tels systèmes sont utilisés pour mener des engagements sur de longues distances, comme ceux des forces spéciales. Ils servent en règle générale à l'exploration en Suisse et dans les régions limitrophes. Les capteurs actuels de l'armée ne sont pas adaptés à cet effet.

La menace émanant de systèmes agissant de manière autonome et de drones téléguidés s'est accrue. L'armée ne dispose pas aujourd'hui de la capacité de s'affirmer dans l'espace électromagnétique contre ces formes de menaces. Cette capacité doit être nouvellement développée.

À l'heure actuelle, l'armée n'emploie aucune arme à haute énergie utilisant les émissions électromagnétiques comme arme. Quant à la question de savoir si l'armée doit développer une telle capacité, il faut la clarifier sur le fond. Les effets directs ou indirects obtenus par ces armes en fonction de la fréquence et de la méthode de rayonnement ne peuvent que difficilement être contrôlés. L'engagement de telles armes dans un environnement densément peuplé peut s'accompagner ainsi d'importants dommages collatéraux. C'est la raison pour laquelle l'armée doit aussi examiner la question de savoir, sur le plan du droit international, quels sont les types de systèmes d'armes, parmi ces derniers, qui pourraient entrer en ligne de compte pour elle, et dans quelle

mesure. Se pose aussi dans ce contexte la question des concepts de protection possibles pour les personnes et les systèmes dans le cadre de la capacité d'autoprotection.

5.8 Capacité Actions dans le cyberespace



5.8.1 Description

En menant des actions dans le cyberespace, on peut empêcher un acteur adverse d'obtenir un avantage en termes de savoir et de prise de décision. On peut en outre entraver ou complètement empêcher le fonctionnement de ses systèmes d'armes. Pour ce faire, il faut que les lacunes sécuritaires et les possibilités d'accès soient connues et que des outils spécifiques soient disponibles, afin de générer les effets visés dans les systèmes en question. Les capacités de mener des actions dans le cyberespace peuvent aussi servir à mettre en œuvre des mesures dans les systèmes TIC propres, afin d'identifier les objectifs et les intentions des acteurs adverses qui y auraient pénétré. Les actions dans le cyberespace et dans l'espace électromagnétique peuvent se combiner sur le plan technique. Les synergies qui en résultent mènent à de nouvelles possibilités pour lutter efficacement contre des systèmes adverses.

5.8.2 Aspect futur

Aujourd'hui, les capacités de mener des actions dans le cyberespace sont avant tout le fait du renseignement. Les actions visant des cibles militaires ont été jusqu'ici plutôt en retrait et doivent à l'avenir être mieux préparées. Afin de pouvoir mener des actions dans le cyberespace, l'armée doit s'adapter rapidement et de manière autonome aux besoins des bénéficiaires de prestations, aux mesures de protection des systèmes cibles et aux nouvelles technologies. En fait partie la capacité de développer des outils de manière autonome et de les engager de manière ciblée. Il faut de plus des cyberteams spécialisés pour appuyer les troupes terrestres ou les forces aériennes. L'appui à l'engagement de ces formations avec des actions dans le cyberespace doit pouvoir être intégré dans le contexte hybride et urbain.

Une lacune capacitaire existe dans l'exploration et l'impact contre des systèmes militaires. Il s'agit ici notamment d'explorer la construction, le fonctionnement et les points faibles par exemple de systèmes d'armes militaires et de les limiter dans leurs fonctionnalités, voire de les rendre inutilisables. La pénétration des systèmes reposant sur des liaisons de données par radio ou sur une connexion à un réseau peut éventuellement se faire à travers cette liaison. Selon les circonstances, l'accès direct à un système cible est nécessaire sur les lieux de l'engagement, ce qui présuppose en règle générale la collaboration avec des troupes adéquates (p. ex. forces spéciales).

Les actions menées dans le cyberespace permettant d'explorer ou d'entraver des systèmes militaires adverses conduisent à un fort élargissement du spectre capacitaire de l'armée. Il s'agit d'être en mesure de mettre hors service à distance des systèmes d'armes ou de conduite, avec une grande précision, et de rechercher des informations. Dans le même temps, on peut éviter des dommages collatéraux pour les êtres humains et les infrastructures. En engagement combiné avec des actions au sol ou dans les airs, les actions dans le cyberespace complètent, appuient et renforcent nettement les impacts des troupes terrestres ou des forces aériennes. Selon les instruments utilisés, on obtient même des effets réversibles, en utilisant par exemple un logiciel de cryptage (rançongiciel). De tels outils permettent de rétablir facilement les données une fois que l'objectif militaire de l'engagement est atteint. Comme pour les actions dans l'espace électromagnétique, de tels moyens agissent par ailleurs à distance. Le risque pour les propres troupes est donc plus faible que si elles devaient combattre les objectifs militaires à l'aide d'armes conventionnelles. Étant donné qu'aucun dommage collatéral ne serait provoqué, contrairement à ce qui aurait été le cas avec une arme, les cybermoyens se prêtent particulièrement bien pour des emplois proportionnés dans des zones bâties et habitées comme le Plateau suisse.

Afin d'atteindre les objectifs lors d'un engagement, il peut être nécessaire de combiner les actions dans le cyberespace et dans l'espace électromagnétique. Les actions dans le cyberespace peuvent par exemple requérir l'accès à des systèmes qui communiquent exclusivement par radio. Dans un tel cas de figure, la liaison radio est utilisée pour pénétrer dans le système cible à travers une cyberattaque.

Ces actions combinées doivent en règle générale être conçues isolément pour chacune des cibles, avec beaucoup d'efforts. Or les solutions techniques développées à cet effet ne peuvent souvent être utilisées ultérieurement pour d'autres emplois qu'au prix de certaines adaptations. De telles actions sont conçues par des équipes composées de spécialistes bien formés issus des domaines de la cryptologie, des cyberactions et de la guerre électronique. La plupart du temps, ces équipes sont complétées par des spécialistes issus d'autres parties de l'armée, par exemple des forces spéciales ou des forces aériennes. De tels engagements nécessitent une préparation étendue et des systèmes d'engagement à haut degré d'automatisation.

5.9 Nécessité d'agir

Autoprotection CYBEEM

L'extension de l'autoprotection CYBEEM doit être au centre du développement visé. Le but est de pouvoir protéger aussi de manière décentralisée les systèmes temporairement mis en réseau et les infrastructures importantes, de garantir la sécurité dans la chaîne d'approvisionnement et d'étendre la capacité d'anticiper les menaces. Il faut de plus améliorer la résilience des centrales d'opération chargées de l'autoprotection CYBEEM. Il faut enfin développer la capacité à durer sur le plan du personnel de manière à ce que l'armée soit en mesure de gérer simultanément plusieurs attaques émanant du CYBEEM.

Capacités d'appuyer la numérisation

Dans la perspective de la compréhension commune de la situation, il faut développer les capacités tout spécialement dans le domaine de la science des données, de l'automatisation et de la représentation de la situation. Il est prévisible que des solutions techniques modernes vont simplifier l'interaction entre l'homme et le système à l'avenir. S'agissant de la collaboration avec des partenaires, il faut créer les conditions préalables nécessaires sur le plan juridique et technique, ou les consolider là où elles existent déjà.

Afin que la résilience dans le traitement des données puisse être assurée pour la troupe à l'engagement également, il faut acquérir l'infrastructure (mobile) de numérisation nécessaire à cet effet. Des normes communes doivent par ailleurs être définies et imposées à l'avenir. Globalement, il s'agit d'établir une conduite TIC plus fortement axée sur les besoins opérationnels de l'armée.

Afin de créer les conditions préalables nécessaires sur le plan technique et organisationnel à une conduite conjointe numérisée, il est nécessaire d'aménager les futurs systèmes de conduite de sorte qu'un flux constant de données soit possible.

Actions dans le CYBEEM

Pour mener des actions dans le CYBEEM, il faut dans tous les cas développer la capacité d'anticiper de futures évolutions (combinée à la cryptologie). Cela vaut en particulier pour l'anticipation de l'évolution technologique et de la menace. Cela présuppose un renforcement majeur de la capacité à implémenter de nouvelles possibilités technologiques dans l'environnement des systèmes existant. Il faut par ailleurs améliorer la capacité d'identifier, analyser et compenser les contre-mesures techniques prises en réaction aux actions propres.

6

Développement et mise en œuvre

Les options de développement de l'Armée suisse dans le CYBEEM doivent s'intégrer dans le système global. Elles tiennent compte des développements capacitaires à venir dans les autres espaces d'opération et les renforcent ou les complètent. Il convient de souligner que le développement capacitaire dans le cyberespace, en particulier, dépend plus de l'augmentation du nombre de spécialistes du domaine que de la mise en place de nouveaux systèmes.

6 Développement et mise en œuvre

Il n'est possible de planifier et de mettre en œuvre des mesures de manière cohérente que si l'on sait précisément dans quelle direction les différentes capacités, qui ont été harmonisées entre elles, doivent être développées. L'aménagement des capacités CYBEEM doit à cet égard en permanence être coordonné avec le développement du système global que constitue l'armée. Les options décrites ci-après tiennent compte de la manière avec laquelle les capacités sont développées dans les autres espaces d'opération et de la manière avec laquelle les moyens sont renouvelés.

6.1 Cadre et paramètres-clés du développement des options

Toutes les options de développement doivent dûment tenir compte des aspects personnels, financiers, juridiques et technologiques. Les projets TIC en cours revêtant de l'importance du point de vue du CYBEEM (p. ex. FITANIA).

Même si les conditions-cadres seront plus difficiles à l'avenir, il reste une certaine marge de manœuvre pour de nouvelles options. Grâce à des solutions technologiques, en particulier l'automatisation, des formations non spécialisées peuvent par exemple aussi être formées pour mener des activités dans le CYBEEM. Si l'armée se focalise sur l'exploitation de ses propres TIC militaires, des fonctions existantes au sein de l'administration militaire peuvent être réorientées sur de nouvelles tâches, tout en sachant que les effets cyber ne se fondent pas prioritairement sur des systèmes militaires coûteux. Ils dépendent avant tout du nombre de spécialistes qui sont disponibles et du type de savoir qu'ils véhiculent.

S'agissant du développement des capacités, il faut tenir compte du fait qu'il y a actuellement des tensions dans certaines parties du CYBEEM, ce qui signifie que des cyberattaques doivent être maîtrisées aujourd'hui déjà ou que des mesures doivent être prises contre l'exploration radio de tiers. C'est pourquoi les options doivent également s'inspirer de menaces aiguës et réelles.

6.2 Mesures à mettre en œuvre dans toutes les options

Différentes mesures doivent être mises en œuvre indépendamment de l'option choisie. Si ce n'était pas le cas, l'exécution future des missions de l'armée serait fondamentalement mise en péril. Il est nécessaire d'agir en particulier pour ce qui concerne l'autoprotection CYBEEM, la numérisation et les capacités à mener des actions dans le CYBEEM.

Autoprotection CYBEEM

S'agissant de l'autoprotection CYBEEM, toutes les options prévoient de créer dans les années à venir les conditions préalables nécessaires à une surveillance complète et à l'échelle de l'armée de ses propres moyens TIC. Cela concerne à la fois des éléments individuels (p. ex. systèmes d'armes disposant d'une composante TIC) et des champs partiels entiers (p. ex. spectre électromagnétique). La partie centrale de l'infrastructure (centrales d'opération) doit à l'avenir disposer d'emplacements de remplacement.

Afin d'améliorer l'autoprotection CYBEEM, il est en outre nécessaire de renforcer les capacités de compréhension de la situation et d'anticipation des évolutions et des menaces futures. Pour renforcer l'autoprotection CYBEEM, il faut également développer la capacité du brouillage radio, avant tout sur le plan du personnel. Si certaines parties des TIC sont séparées du réseau global, il faut des prestations de protection décentralisées. Quant à la capacité de l'armée de contrôler sa propre image des émissions dans l'espace électromagnétique, elle doit être mise en place intégralement, au même titre

d'ailleurs que la sécurité de la chaîne d'approvisionnement, qui fait aujourd'hui encore complètement défaut à l'armée. Or, afin que ces tâches puissent être accomplies en permanence, l'administration militaire doit être adaptée.

Capacités d'appuyer la numérisation

Une situation peut être comprise dans son intégralité lorsque des informations sur la situation provenant de tous les espaces d'opération et de tous les domaines fonctionnels de l'armée et des partenaires sont compilées et fusionnées. Pour rendre cela possible, il faut que les données requises soient préparées et présentées de manière automatisée. Il faut de plus une capacité à planifier et piloter les flux d'informations en fonction de la mission et de la situation, avec l'appui de technologies issues du domaine de la science des données. Les capacités déjà existantes au niveau de la science des données seront élargies en collaboration avec le Centre de compétences en science des données (DSCC) de l'Office fédéral de la statistique (OFS). Dans un premier temps, il s'agira d'augmenter le nombre de spécialistes. Dans un second temps, à la fin des années 2020, l'infrastructure informatique sera étendue pour répondre aux besoins de la science des données conformément au programme FITANIA.

Le programme FITANIA constitue la base technique nécessaire à un traitement robuste et sûr des données et au réseau intégré de conduite numérique de l'armée. La troupe doit en outre être habilitée à utiliser les possibilités de transmission civiles éventuellement disponibles en redondance avec les options militaires. Afin d'assurer la capacité robuste de commandement et de collaboration de la troupe lors de ses engagements, celle-ci doit disposer de plateformes TIC locales standard, capables d'être mises en réseau et offrant des postes de travail équipés. Cela permet de réduire la variété des plateformes du réseau intégré de conduite numérique et d'en simplifier l'exploitation.

Sur ces plateformes en réseau, les états-majors des troupes utilisent les services TIC pour diriger, pour gérer les données et pour accomplir d'autres tâches. En outre, cela crée également la possibilité de raccorder des systèmes d'engagement et des partenaires.

De plus, les futurs moyens TIC et applications de conduite militaire doivent être aménagés de sorte que les données puissent être échangées facilement. Ceci crée une condition supplémentaire nécessaire à une conduite numérique conjointe. Pour ce faire, l'intégration doit être garantie sur le double plan organisationnel et technique, au niveau des processus, du flux d'informations et du système.

Le réseau intégré de conduite numérique ne cesse d'être développé avec l'ajout de systèmes de capteurs, de conduite et d'armes. En cas de mise en réseau avec des partenaires internes et externes, il faut définir la forme de collaboration et les interfaces s'y rapportant. Cette collaboration a par ailleurs besoin d'un système régulatoire transorganisationnel (gouvernance).

Actions dans le cyberespace et l'espace électromagnétique

Pour pouvoir agir dans le cyberespace et l'espace électromagnétique, l'armée doit être en mesure d'anticiper les évolutions[128] et les menaces technologiques futures, ceci en intégrant des capacités cryptologiques. C'est la seule manière de répondre rapidement aux nouveaux besoins de l'armée et du SRC. On renforce ainsi la capacité d'implémenter de nouvelles solutions technologiques et de compenser les contre-mesures. L'infrastructure TIC spécialisée nécessaire fait partie de l'infrastructure de la science des données. Il faut par ailleurs poursuivre le développement de la capacité de déployer des capteurs mobiles et aériens. L'infrastructure servant à l'exploration radio stratégique doit être aménagée de manière redondante dans certains secteurs importants. Enfin, il s'agit de préserver les capacités de mener la guerre électronique au profit de

128 Le monitorage de l'évolution technologique s'effectue en collaboration avec des partenaires au sein du DDPS.

l'espace aérien et de les développer en tenant compte des acquisitions futures, telles que prévues dans le programme Air2030.

Les options décrites ci-après fixent des points forts qualitativement et quantitativement différents pour ce qui est des capacités dans le cyberespace d'un côté et de celles dans l'espace électromagnétique de l'autre. Elles illustrent comment les capacités CYBEEM peuvent évoluer, dans la profondeur et la largeur.

6.3 Option 1

Avec l'option 1, l'armée renforcerait en particulier l'autoprotection dans le cyberespace et l'espace électromagnétique. Cette autoprotection serait par principe assurée de manière centralisée, raison pour laquelle les capacités requises, qualitativement élevées, seraient comme aujourd'hui regroupées dans un bataillon spécialisé à l'échelon de l'armée. Une protection décentralisée ponctuelle jusqu'à l'échelle des bataillons et des compagnies serait en outre possible. Pour ce faire, des moyens adaptés issus du bataillon spécialisé pourraient être affectés ou subordonnés aux formations de combat de l'armée (ou à des partenaires civils si nécessaire).

Après la mise en œuvre de cette option, elles disposeraient de la capacité de développer et de mener simultanément et intégralement plusieurs actions contre des objectifs militaires. Les troupes chargées des engagements militaires dans le CYBEEM et de l'autoprotection décentralisée seraient regroupées dans des bataillons spécialisés au niveau de l'armée, par analogie aux divisions GE existantes et au bataillon cyber.

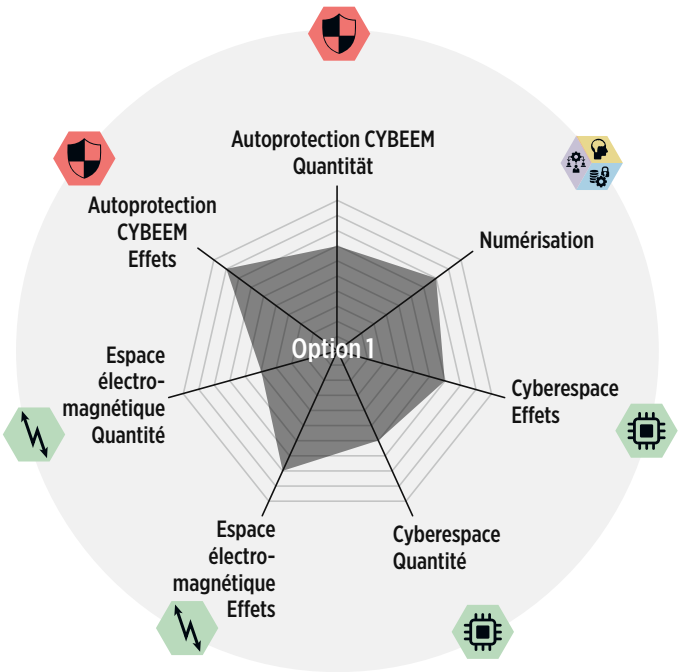


Illustration 14 : étendue des capacités de l'option 1

6.3.1 Prestations

Autoprotection CYBEEM

La mise en œuvre de cette option permettrait de protéger des infrastructures importantes de manière décentralisée et ponctuelle. Pour ce faire, des moyens issus d'un bataillon spécialisé à l'échelon de l'armée pourraient être affectés ou subordonnés en fonction des besoins à d'autres formations de l'armée (ou à des partenaires civils si nécessaire).

Capacités d'appuyer la numérisation

La troupe serait équipée d'une infrastructure TIC mobile jusqu'à l'échelon du bataillon, afin de pouvoir traiter les données de manière indépendante et éventuellement autonome. Les conditions préalables nécessaires à une conduite numérique conjointe seraient ainsi créées jusqu'à cet échelon.

Actions dans l'espace électromagnétique

S'agissant des actions dans l'espace électromagnétique, le développement autonome de signaux électromagnétiques serait renforcé pour les engagements. Afin de pouvoir fournir des efforts principaux ou assurer la liberté de manœuvre, des bataillons spécialisés seraient disponibles à l'échelon de l'armée.

Actions dans le cyberespace

Les capacités de l'armée de mener des actions dans le cyberespace seraient renforcées. Les outils nécessaires seraient largement développés par l'armée elle-même, ce qui lui permettrait d'améliorer sa capacité à impacter des systèmes cibles militaires. L'armée serait ainsi en mesure de planifier simultanément plusieurs attaques contre les systèmes d'un adversaire, de développer les outils nécessaires et de mener les engagements ad hoc. La capacité d'exécuter des analyses de composantes TIC (p. ex. supports de données trouvés) serait par ailleurs mise en place au sein des troupes. Un bataillon spécialisé serait prévu à cet effet, qui pourrait soutenir d'autres troupes à l'aide d'actions militaires ponctuelles dans le cyberespace et exécuter la forensique dans le secteur d'engagement.

6.3.2 Investissements nécessaires

Les investissements nécessaires à l'option 1 se situeraient aux alentours de 1,4 à 2 milliards de francs. L'effectif en personnel resterait lui inchangé. L'effectif en personnel de milice découle du besoin de disposer de spécialistes et de militaires exerçant deux fonctions, assumant ainsi des tâches dans le domaine de la cyberdéfense en plus de leur fonction principale. Il se monte au total à environ 5000 à 6000 militaires. Au total, parmi toutes les options examinées, l'option 1 est celle qui exige le moins de ressources financières et en personnel.

6.3.3 Avantages et inconvénients

L'option 1 se fonde sur les projets en cours (p. ex. FITANIA). La partie centrale de l'autoprotection CYBEEM serait aménagée de manière redondante. Des moyens seraient en outre créés qui permettraient d'étendre la protection de manière ponctuelle et décentralisée. La base technique de la capacité de la conduite de l'armée serait ainsi nettement mieux protégée qu'aujourd'hui.

Les conditions techniques préalables nécessaires à une conduite numérique permettraient d'augmenter la vitesse lors d'un engagement. Des technologies modernes seraient utilisées jusqu'à l'échelon du bataillon (p. ex. réalité augmentée dans la logistique ou auprès des forces d'engagement).

Dans l'option 1, les capacités du secteur de la science des données seraient aménagées de sorte à pouvoir être utilisées dans l'ensemble de l'armée. Cela renforcerait la compréhension commune de la situation pour toute l'armée. L'indépendance de l'armée dans le cyberespace et dans l'espace électromagnétique serait développée de telle manière qu'elle ne devrait plus que ponctuellement recourir à des tiers. L'armée serait ainsi plus flexible et autonome, tout en augmentant sa marge de manœuvre. L'infrastructure partiellement redondante améliorerait de plus la résilience de l'exploration radio stratégique.

Avec la mise en œuvre de l'option 1, la troupe pourrait être soutenue à l'engagement par des effets CYBEEM jusqu'à l'échelon du bataillon, de manière toutefois limitée et

priorisée par l'échelon de l'armée. Le besoin en capacités découlant de l'image hybride des conflits ne serait ainsi que partiellement couvert.

Le principal désavantage de l'option 1 réside dès lors dans la capacité réduite d'appuyer les troupes à l'engagement à l'aide d'effets cyber et électromagnétiques. Avec les formations disponibles à son niveau, l'échelon de l'armée ne pourrait que former des points forts limités dans le temps. De plus, la capacité de densifier l'autoprotection CYBEEM de manière décentralisée ne serait que ponctuellement disponible.

6.4 Option 2

Avec l'option 2, la majorité des bataillons et des compagnies sera intégralement habilitée à mener des actions autonomes dans le CYBEEM et à assurer de manière indépendante l'autoprotection CYBEEM. Ces formations seraient complétées par des spécialistes et par les systèmes nécessaires. Des bataillons spécialisés pour des engagements dans le cyberespace et dans l'espace électromagnétique seraient par ailleurs disponibles à l'échelon de l'armée. L'armée ne disposerait de capacités propres dans le cyberespace et dans l'espace électromagnétique que dans les domaines-clés. Elle aurait à cet égard besoin du soutien de l'industrie.

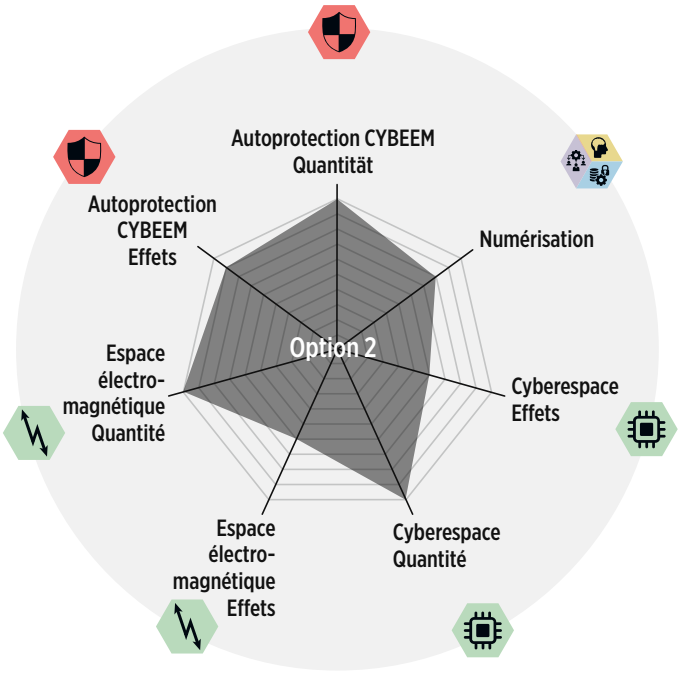


Illustration 15 : étendue des capacités de l'option 2

6.4.1 Prestations

Autoprotection CYBEEM

Dans l'option 2, la majorité des bataillons et des compagnies sera dotée de spécialistes et de systèmes chargés de l'autoprotection CYBEEM, qui pourraient assurer la protection décentralisée. Ces formations seraient ainsi en mesure de protéger leurs systèmes TIC de manière autonome dans le secteur d'engagement. Un bataillon spécialisé serait par ailleurs formé à l'échelon de l'armée pour la constitution de points forts.

Capacités d'appuyer la numérisation

Comme dans l'option 1, la troupe serait équipée d'une infrastructure TIC mobile jusqu'à l'échelon du bataillon, afin de pouvoir traiter les données de manière indépendante et éventuellement autonome. Les compagnies seraient par ailleurs également dotées

de systèmes réduits. Les conditions préalables nécessaires à une conduite numérique conjointe seraient ainsi créées jusqu'à cet échelon de conduite inférieur.

Actions dans l'espace électromagnétique

Pour les actions dans l'espace électromagnétique, le développement autonome de signaux électromagnétiques serait renforcé pour les engagements. Des bataillons spécialisés chargés des actions militaires dans l'espace électromagnétique seraient par ailleurs disponibles à l'échelon de l'armée. Ceux-ci disposeraient également de moyens de défense sol-air pour perturber des systèmes radars adverses. Les formations à l'échelon de l'armée serviraient à constituer des points forts et à préserver la liberté d'action.

Dans l'option 2, la majorité des bataillons et des compagnies disposeraient de spécialistes propres et de systèmes pour mener des actions dans l'espace électromagnétique. Ces systèmes devraient afficher un degré d'automatisation élevé, afin que la troupe puisse les engager facilement. Ils ne seraient toutefois pas particulièrement bien protégés contre les effets des armes conventionnelles.

Actions dans le cyberespace

Les capacités de l'armée de mener des actions dans le cyberespace seraient certes également développées dans cette option, à un niveau qualitativement plus bas cependant que dans l'option 1. En revanche, de très nombreux bataillons et compagnies pourraient être dotés de moyens leur permettant de procéder à des actions autonomes dans le cyberespace. Afin de pouvoir développer des outils et des procédures d'attaque, l'armée aurait en règle générale besoin de l'appui de l'industrie.

À l'échelon de l'armée, un bataillon spécialisé serait disponible pour constituer des points forts ou assurer la liberté d'action. Comme pour les actions dans l'espace électromagnétique, la majorité des bataillons et des compagnies disposeraient qui plus est de spécialistes propres et des systèmes nécessaires. Ces systèmes seraient également hautement automatisés, afin de pouvoir être utilisés facilement par la troupe.

Automatisation

La disponibilité technique à l'engagement doit au quotidien déjà être continuellement adaptée aux dernières évolutions, ce qui nécessite d'expérience plusieurs mois, voire années. Les systèmes ne peuvent donc pas seulement être acquis et introduits auprès de la troupe peu de temps avant un engagement. Afin de pouvoir garantir la disponibilité technique à l'engagement des systèmes, un domaine particulier serait créé au niveau de l'administration militaire dans l'option 2.

6.4.2 Investissements nécessaires

Les investissements nécessaires à l'option 2 se situeraient entre 2 et 2,6 milliards de francs environ. L'option 2 serait donc plus coûteuse que l'option 1, avant tout parce qu'un grand nombre de systèmes devraient être acquis pour équiper les bataillons et les compagnies. L'effectif en personnel resterait lui inchangé. L'effectif en personnel de milice serait pour sa part de 7000 à 8000 militaires. Il s'agirait avant tout de spécialistes CYBEEM et de militaires exerçant deux fonctions assumant des tâches dans le domaine de la cyberdéfense en plus de leur fonction principale. S'agissant du nombre de systèmes, l'option 2 entraînerait le développement de capacités le plus étendu. C'est pourquoi il s'agit aussi de l'option qui nécessite le plus de ressources, à la fois pour ce qui est des investissements ainsi que du personnel professionnel et de milice indispensable à la mise en œuvre.

6.4.3 Avantages et inconvénients

L'option 2 se fonde sur les projets en cours, comme ceux qui sont réalisés avec le programme FITANIA. Les principales différences par rapport à l'option 1 se situent au niveau de l'aménagement de l'autoprotection CYBEEM et des actions dans le CYBEEM.

L'autoprotection CYBEEM décentralisée serait fortement étendue et un grand nombre de moyens seraient acquis. L'armée pourrait ainsi aussi protéger la majorité de son infrastructure TIC lorsque celle-ci serait séparée du réseau global. Les capacités de mener des engagements dans le cyberespace et l'espace électromagnétique seraient avant tout nettement développées pour ce qui concerne le nombre de systèmes. Des bataillons spécialisés seraient par ailleurs disponibles pour constituer des points forts à l'échelon de l'armée.

La force de l'option 2 réside dans le fait que ce seraient essentiellement les troupes terrestres qui seraient habilitées à mener des actions simples dans le cyberespace et dans l'espace électromagnétique. Grâce à l'autoprotection CYBEEM décentralisée largement développée, la capacité technique à la conduite de l'armée serait en outre intégralement protégée. Une telle protection intégrale serait une réponse adéquate à la menace spécifique telle qu'elle découle du possible conflit hybride mené par un adversaire. L'échelon de l'armée gagnerait de plus nettement en liberté d'action dans ce domaine. Par rapport aux autres options se pose néanmoins la question de savoir si l'effet de protection additionnel obtenu justifie le déploiement nettement plus important de moyens qui serait nécessaire pour la mise en œuvre de cette option.

L'exploitation, l'entretien et l'automatisation du très grand nombre de systèmes exigeraient beaucoup de personnel professionnel. Ces spécialistes feraient toutefois ensuite défaut lorsqu'il s'agirait de planifier et d'exécuter avant tout des actions exigeantes dans le cyberespace contre des objectifs militaires à plus haute valeur et mieux protégés.

L'important développement des éléments CYBEEM aurait un impact en termes de personnel sur d'autres corps de troupe, car il devrait avoir lieu au détriment d'autres parties de l'armée, puisque les effectifs totaux de l'armée, eux, ne changeraient pas. Le nombre de spécialistes nécessaires à l'administration militaire serait élevé et ne pourrait probablement être recruté sur le marché suisse qu'à grands frais. De nombreux nouveaux systèmes devraient par ailleurs être acquis, ce qui entraînerait des coûts additionnels.

Certains risques existent également dans le domaine de la technologie. L'acquisition de systèmes déployant des effets automatisés dans le cyberespace pour les formations de l'échelon tactique inférieur constituerait un défi tout particulier. Il faudrait acquérir de nombreux moyens qui, en raison de leur construction de base et de l'évolution technologique, ne pourraient pas être modernisés et seraient par conséquent probablement inadaptés à un engagement futur. Ils devraient donc être renouvelés à intervalles réduits, ce qui rendrait le maintien des capacités plus coûteux.

6.5 Option 3

L'option 3 vise à ce que l'armée soit capable à l'avenir se protéger intégralement contre les attaques provenant du CYBEEM. La protection se rapporte à des systèmes exploités aussi bien en permanence que temporairement (p. ex. systèmes d'armes disposant d'une importante partie TIC). L'autoprotection contre les menaces issues de l'espace électromagnétique serait en particulier nettement plus étendue que dans les autres options. Celle-ci serait assurée de manière centralisée, les capacités hautement qualitatives requises à cet effet étant regroupées dans un bataillon spécialisé à l'échelon de l'armée, par analogie avec le bataillon cyber créé pour le début de l'année 2022. Une protection ponctuelle décentralisée d'infrastructures importantes serait toutefois également possible. Pour ce faire, des moyens issus du bataillon cyber pourraient être affectés ou subordonnés en fonction des besoins à d'autres formations de l'armée (ou à des partenaires civils si nécessaire).

Outre l'autoprotection, des mesures actives seraient également prises dans le domaine cyber, afin que l'armée puisse se défendre de manière appropriée contre les me-

naces, également celles provenant d'un système d'armes adverse (p. ex. les systèmes de conduite et de pilotage de l'artillerie à longue portée ou les systèmes de défense sol-air). Cette option prévoit à cet égard le développement de capacités permettant de planifier et d'exécuter simultanément et intégralement plusieurs attaques exigeantes contre des objectifs militaires.

Avec l'option 3, l'armée placerait un point fort sur l'impact et l'autoprotection dans l'espace électromagnétique. Dans ces domaines, la majorité des bataillons et des compagnies seraient habilités à exécuter des engagements autonomes et dotés pour ce faire des systèmes nécessaires, faciles à utiliser. Les formations seraient ainsi en mesure d'étouffer de manière autonome l'échange adverse de données par radio dans leur secteur d'engagement et d'entraver la capacité adverse à la conduite à l'échelon tactique également. À l'engagement, les formations de combat pourraient dès lors compenser l'absence de cybermoyens propres. Pour les engagements plus importants dans l'espace électromagnétique, un petit nombre de corps de troupe spécialisés serait par ailleurs formé et développé, par analogie avec les deux divisions GE déjà existantes.

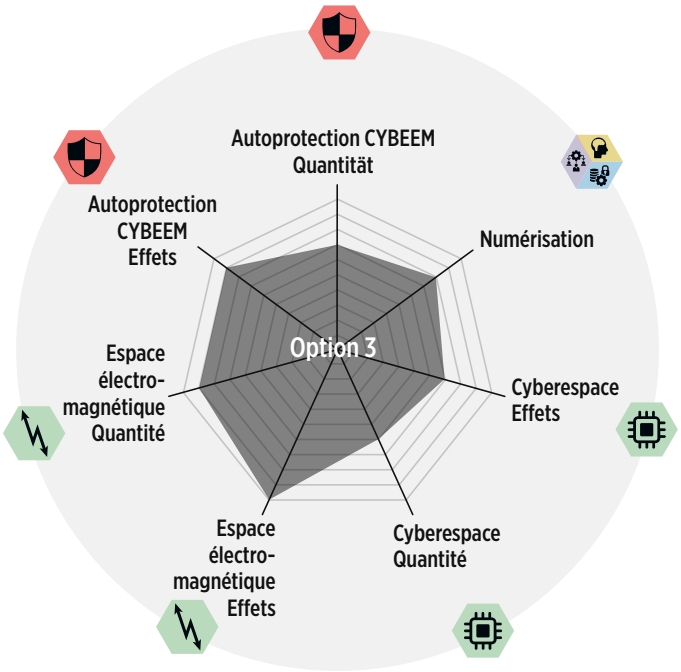


Illustration 16 : étendue des capacités de l'option 3

6.5.1 Prestations

Autoprotection CYBEEM

S'agissant de l'autoprotection CYBEEM, il n'y a pas de différence avec l'option 1. En particulier, il serait possible d'assurer une protection ponctuelle décentralisée d'infrastructures importantes. Pour ce faire, des moyens issus du bataillon cyber pourraient être affectés ou subordonnés en fonction des besoins à d'autres formations de l'armée (ou à des partenaires civils si nécessaire).

Capacités d'appuyer la numérisation

S'agissant de l'appui à la numérisation, il n'y a pas non plus de différence avec l'option 1. La troupe serait équipée d'une infrastructure TIC mobile jusqu'à l'échelon du bataillon, afin de traiter les données de manière indépendante et éventuellement autonome. Les conditions préalables nécessaires à une conduite numérique conjointe seraient ainsi créées jusqu'à cet échelon.

Actions dans l'espace électromagnétique

Comme dans l'option 1, le développement autonome de signaux électromagnétiques pour les engagements serait renforcé pour les actions dans l'espace électromagnétique. Des bataillons spécialisés à l'échelon de l'armée seraient disponibles pour constituer des points forts et préserver la liberté d'action. Comme dans l'option 2, ceux-ci disposeraient également de moyens de défense sol-air pour perturber les systèmes radars adverses.

Des spécialistes propres et les systèmes nécessaires seraient par ailleurs affectés à la majorité des bataillons et des compagnies. Les plateformes d'armes (p. ex. chars) de ces formations disposeraient dans l'espace électromagnétique de systèmes d'autoprotection et d'impact hautement automatisés et intégrés.

Actions dans le cyberespace

Pour mener des actions dans le cyberespace, les capacités de l'armée seraient développées comme dans l'option 1. L'armée développerait les outils nécessaires de manière largement autonome et améliorerait ainsi sa capacité à agir contre des systèmes militaires cibles. Elle serait de cette manière en mesure de planifier simultanément plusieurs attaques contre des systèmes adverses et de conduire les engagements ad hoc. Les troupes seraient par ailleurs dotées de la capacité de mener des analyses de composantes TIC (p. ex. supports de données trouvés). Un bataillon spécialisé serait prévu à cet effet, qui pourrait appuyer d'autres troupes par des actions militaires ponctuelles dans le cyberespace et exécuter la forensique dans le secteur d'engagement.

6.5.2 Investissements nécessaires

Les investissements nécessaires à l'option 3 se situeraient aux alentours des 1,6 à 2,4 milliards de francs, soit entre les options 1 et 2. Le besoin en investissements découle avant tout de l'acquisition des moyens pour l'appui à l'engagement des bataillons et des compagnies. L'effectif en personnel resterait quant à lui inchangé. S'agissant du personnel de milice, il faudrait avant tout recruter des spécialistes CYBEEM additionnels et des militaires exerçant deux fonctions. Le besoin en personnel de milice se situerait pour sa part entre 6000 et 7000 militaires, soit entre les deux autres options également.

6.5.3 Avantages et inconvénients

L'option 3 se fonde également sur les projets en cours, tels que FITANIA. S'agissant de la compréhension commune de la situation et du traitement robuste et sûr des données, elle correspond à l'option 1. Les capacités de mener des actions dans le CYBEEM seraient également développées. La majorité des formations disposeraient d'éléments leur permettant d'exécuter des actions dans l'espace électromagnétique. Ceci correspond au besoin en capacités découlant du conflit hybride. Les plateformes d'armes dans les formations d'engagement seraient dotées de systèmes électromagnétiques intégrés d'autoprotection et d'impact. Les moyens servant à l'autoprotection CYBEEM et aux actions dans le cyberespace seraient regroupés à l'échelon de l'armée dans des bataillons spécialisés et pourraient être affectés aux formations de combat en fonction des besoins. Par rapport à l'option 2, nettement moins de formations et d'infrastructures pourraient toutefois être protégées. Afin de constituer des points forts pour des actions dans l'espace électromagnétique, l'échelon de l'armée disposerait de bataillons spécialisés. Celle-ci gagnerait ainsi en liberté d'action. Les moyens pour les actions dans le cyberespace seraient certes réduits et regroupés à l'échelon de l'armée ; cela pourrait toutefois être compensé par le fait que la majorité des bataillons et des compagnies seraient équipés de moyens pour mener des actions dans l'espace électromagnétique. S'agissant des capacités pour conduire des actions dans le cyberespace, c'est la qualité qui primerait. Celle-ci pourrait être augmentée en raison du renoncement à un développement quantitatif intégral.

6.6 Évaluation des options

Chaque option donne des réponses aux exigences découlant de l'évolution des conflits et des progrès technologiques. Toutes les options créent de bonnes conditions pour faire avancer la numérisation au sein de l'armée. Toutes permettent par ailleurs de développer les autres capacités de l'armée, telles qu'elles sont décrites dans les rapports Avenir des forces terrestres et Avenir de la défense aérienne.

Au niveau de l'appréciation globale, l'option 3 est celle qui l'emporte. Elle affiche le meilleur spectre capacitaire et la meilleure performance. Ceci est dû au fait que, dans l'option 3, les capacités CYBEEM sont nettement développées aux différents échelons de conduite, avec des combinaisons diverses. Les moyens permettant de mener des actions dans le cyberespace sont réduits sur le plan du nombre au profit de la qualité et sont regroupés à l'échelon de l'armée. Les faiblesses apparentes qui en découlent pour les bataillons et les compagnies en termes de cyberdéfense sont largement compensées par des moyens permettant de conduire des actions dans l'espace électromagnétique. Ces moyens font que les formations de combat sont en mesure d'étouffer de manière autonome l'échange adverse de données par radio dans leur secteur d'engagement et d'entraver la capacité de conduite adverse à l'échelon tactique également. À l'engagement, les formations peuvent par conséquent largement compenser l'absence de cybermoyens propres. La mise en place de capacités pour mener des actions dans le cyberespace à l'échelon des bataillons et des compagnies n'apporterait qu'une faible utilité militaire supplémentaire et mobiliserait de nombreuses ressources de manière disproportionnée.

Dans l'option 2, la majorité des bataillons et des compagnies disposent certes de capacités propres qualitativement limitées pour exécuter des actions simples dans le cyberespace. Cela mobilise néanmoins des ressources en personnel pour l'automatisation et la disponibilité technique à l'engagement des très nombreux systèmes, ce qui a des répercussions négatives sur la qualité pouvant être atteinte par l'armée dans le cyberespace. L'option 2 est donc moins adaptée que l'option 3 pour poursuivre le développement des capacités CYBEEM de l'armée dans le futur. S'ajoute à cela le fait que, dans l'option 3, l'autoprotection contre les menaces issues de l'espace électromagnétique est nettement plus marquée. Grâce à son profil équilibré et harmonieux de prestations, elle offre de plus le meilleur cadre pour réagir de manière flexible aux futurs défis et menaces. Enfin, l'option 3 fait aussi meilleure figure que les autres options pour ce qui est du besoin en personnel, des coûts et du risque technologique et offre donc le paquet d'ensemble le plus équilibré.

6.7 Jalons de la mise en œuvre de l'option 3

Jusqu'au début des années 2030, l'acquisition d'armement va mettre l'accent sur les nouveaux avions de combat et sur les moyens de défense sol-air de longue portée. Il faut également développer de manière adéquate les cybercapacités, l'accent devant être mis sur l'autoprotection CYBEEM. Ensuite, les acquisitions devront à nouveau être réparties plus équitablement entre tous les champs de capacités.

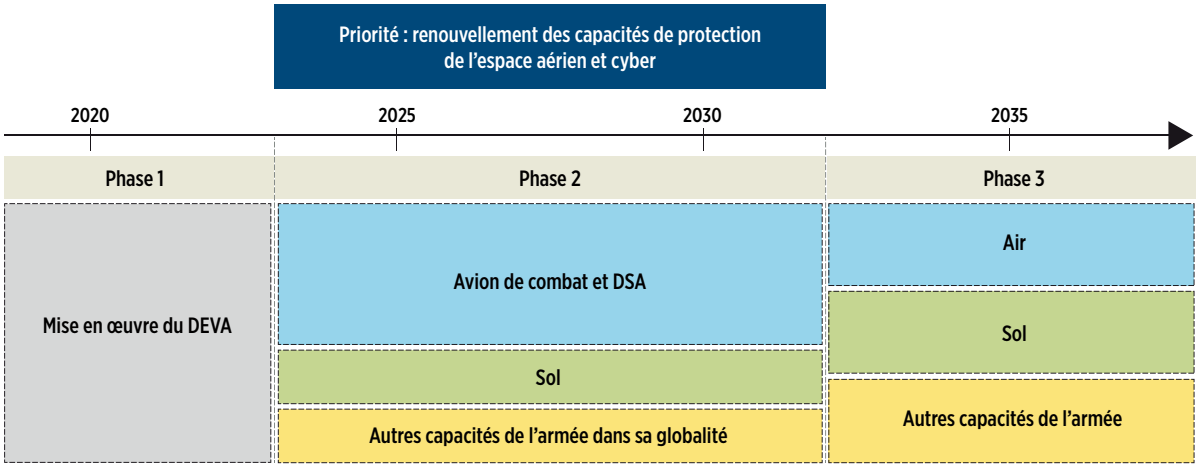


Illustration 17 : points de focalisation des investissements[129]

Jusqu'en 2030, d'autres jalons temporels peuvent déjà être déduits. Les conditions préalables nécessaires à la numérisation de l'armée seront mises en place dans les années 2024-2025, avec la fin de la première migration d'applications sur les deux nœuds nationaux. L'armée va par ailleurs former le commandement Cyber au début de l'année 2024. L'aménagement plein des capacités dans des centres de calcul protégés est lui prévu pour les années 2028-2029. Enfin, les moyens de télécommunication de l'armée vont être remplacés d'ici le début des années 2030 par le projet TC A. Quant à la mise en œuvre de nouveaux projets immobiliers d'envergure, elle devrait être possible à partir de 2028-2029.

Ces jalons temporels entraînent les conséquences suivantes pour la mise en œuvre de cette option :

— La densification du Réseau de conduite suisse décrite dans l'option est prévue à partir de 2030.
— L'aménagement technique de la transmission des données (via fibre optique et radio) est en grande partie garanti avec la conclusion du projet TC A d'ici aux années 2040 ; il constitue un cadre fixe pour la mise en œuvre de cette option.
— L'introduction à large échelle de l'infrastructure de numérisation s'effectue idéalement au terme de la mise en place du réseau de centres de calcul et des nœuds régionaux et locaux dès 2028.
— L'aménagement complet prioritaire de l'infrastructure TIC pour la science des données peut être implémenté au terme de la mise en place du réseau de centres de calcul.
— Les capacités CYBEEM des grands systèmes terrestres (p. ex. autoprotection) ne devraient être mises en œuvre que dans le cadre de leur remplacement prévu au début des années 2030. On peut ainsi éviter des réarmements coûteux de systèmes existants.

6.8 Mise en œuvre

À partir des jalons définis dans le chapitre précédent, on peut déduire grossièrement trois étapes de mise en œuvre et illustrer ainsi un horizon temporel approximatif (cf. illustration 20). Étant donné que certaines mesures sont mises en place sur l'ensemble dudit horizon et qu'il existe des dépendances mutuelles, il n'est pas possible de dissocier clairement les étapes les unes des autres. On se contente donc d'esquisser les mesures qui doivent être mises en œuvre dans chaque étape en guise de point de focalisation principal. Ce procédé permet de déjà évaluer à chaque fois la prochaine étape, de l'adapter en fonction du cadre changeant et de l'aménager si nécessaire selon les éventuelles évolutions technologiques.

129 Cf. rapport Avenir des forces terrestres, p. 131.

Dans l'étape 1, il s'agit de développer les capacités CYBEEM centrales et les capacités à l'échelon de l'armée. Dans l'étape 2, les capacités décentralisées doivent être mises en place jusqu'à l'échelon de conduite tactique inférieur, en partie même jusqu'à l'échelon de conduite de la technique de combat, comme le traitement robuste et sûr des données au sein des bataillons et des compagnies. Un autre point fort de cette étape est le développement de la résilience de l'infrastructure-clé importante pour les engagements au niveau de l'autoprotection CYBEEM. C'est également lors de cette étape que l'organisation des formations est adaptée. Enfin, dans l'étape 3, on peut passer au développement des capacités de mener des actions dans l'espace électromagnétique au sein des formations de manœuvre. D'une part, il faut dans le cadre du renouvellement des systèmes terrestres développer la capacité de l'échelon de la conduite tactique à exercer un impact dans l'espace électromagnétique. D'autre part, il s'agit de continuer à développer la capacité de base à mener des actions dans le cyberespace à l'échelon de l'armée.

Ce procédé doit être choisi, car

— toutes les mesures sont synchronisées avec les projets en cours et tiennent compte du cadre supérieur ;
— l'autoprotection CYBEEM est développée avec une priorité élevée et les conditions techniques préalables nécessaires à la conduite de l'armée sont ainsi garanties ;
— le développement des capacités CYBEEM s'effectue d'abord dans la partie centralisée puis décentralisée ; il en résulte un système global résistant, constant et sûr ;
— ce processus par étapes permet d'adapter à chaque fois la prochaine étape au cadre changeant et de suivre le rythme des éventuelles autres évolutions technologiques ;
— le renouvellement des systèmes terrestres à partir de 2032 est l'opportunité de combiner le développement de la capacité de mener des actions dans l'espace électromagnétique à l'échelon de la conduite tactique avec la nouvelle acquisition de systèmes terrestres, sur un plan technique, et d'utiliser les synergies en découlant.

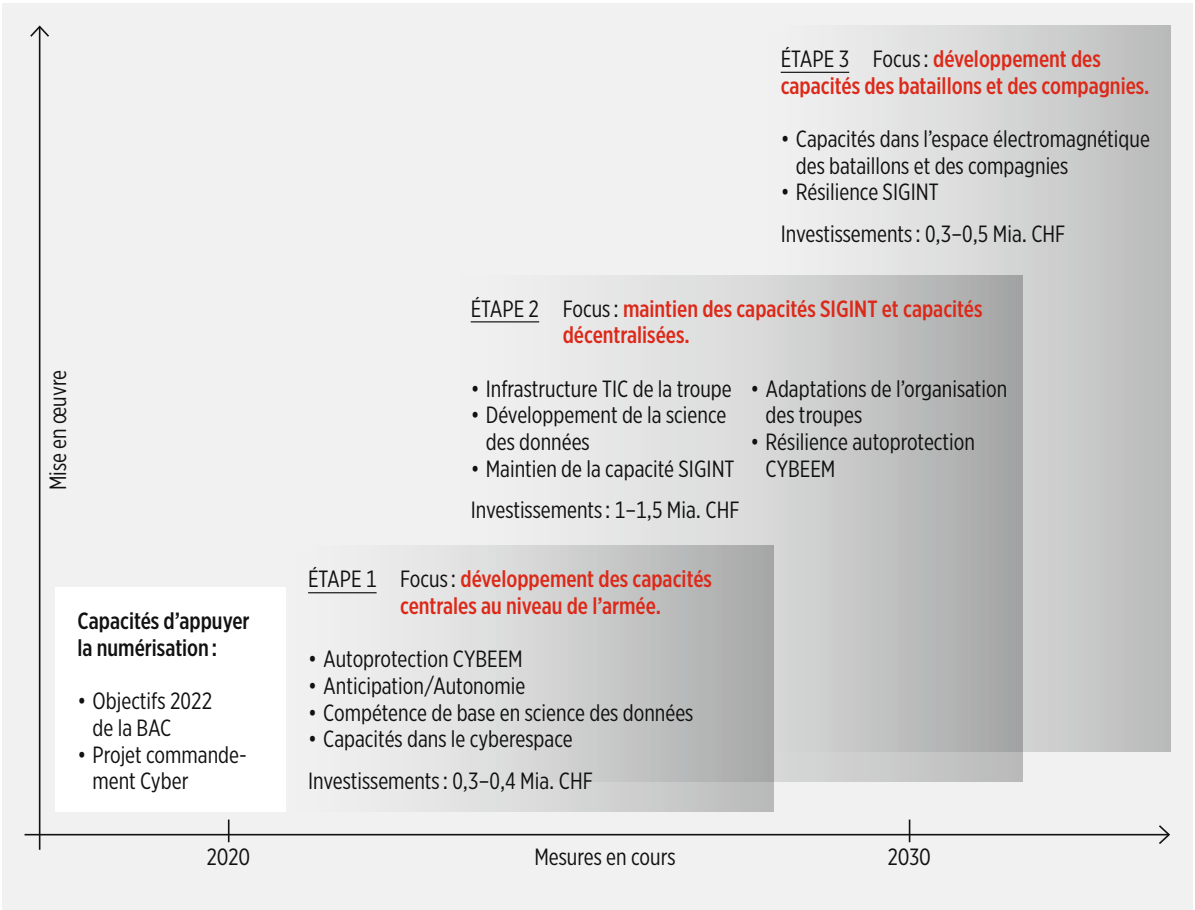


Illustration 18 : étapes de la mise en œuvre de l'option 3

7

Coopération avec des partenaires dans le cadre du RNS et avec des tiers

Par des coopérations dans le domaine Cyber, l'armée participe activement au Réseau national de sécurité (RNS) et appuie les autorités de manière subsidiaire en cas de besoin. Avec son stage de formation cyber, elle contribue en outre à réduire le manque de personnel qualifié en Suisse.

7 Coopération avec des partenaires dans le cadre du RNS et avec des tiers

Plusieurs incidents ont montré ces derniers temps à quel point les infrastructures critiques sont vulnérables vis-à-vis des cyberattaques. La cyberattaque ayant visé le *Colonial-Pipeline* en mai 2021 a par exemple conduit à une interruption de plusieurs jours de l'alimentation en pétrole sur la côte est des États-Unis et provoqué une pénurie étendue en combustibles fossiles. Après peu de temps déjà, cette interruption a eu un impact massif sur l'ensemble de la société de la côte est des États-Unis. Se pose dès lors la question de savoir ce qui se serait passé si cette attaque n'avait pas visé le *Colonial-Pipeline* aux États-Unis, mais par exemple les réseaux de transmission d'électricité en Suisse. En cas d'attaque réussie, l'alimentation électrique du pays aurait été fortement limitée. La conclusion évidente est que les organes responsables recourraient rapidement à toutes les ressources appropriées du pays pour gérer une telle crise, y compris aux spécialistes et aux moyens de l'armée.

Globalement, les coopérations améliorent la qualité des capacités propres à l'armée. L'armée obtient un accès à du savoir spécialisé externe et peut profiter des expériences de tiers. Des interfaces additionnelles recèlent toutefois aussi toujours des risques et de potentiels points faibles. Une collaboration ne se justifie donc que lorsque les capacités sont établies au sein de l'armée. Un développement commun de capacités dans le cadre d'une coopération est également envisageable. Il faut viser un développement priorisé par étapes desdites coopérations.

7.1 Appui subsidiaire

L'armée appuie les autorités civiles de manière subsidiaire sur la base de la loi sur l'armée. Les autorités civiles peuvent demander une aide militaire lorsque leurs moyens sont épuisés ou qu'ils peuvent prouver que les moyens nécessaires ne sont pas disponibles et ne peuvent pas non plus être fournis dans la quantité souhaitée et en temps opportun par des prestataires commerciaux. Après un cyberincident, des éléments de l'armée peuvent ainsi être engagés à la demande des autorités compétentes, afin de maîtriser l'une ou l'autre conséquence de l'incident en question (p. ex. pénurie logistique). Des cyberéléments peuvent par ailleurs être déployés de manière subsidiaire, par exemple pour contribuer à analyser l'incident et à rétablir le bon fonctionnement des services. Pendant tout ce temps, l'armée peut, en concertation avec les autorités compétentes, fournir des prestations dans le domaine de l'appréciation de la cybersituation générale et particulière. Un tel engagement se fait à la demande des autorités civiles.

Il ne serait pas judicieux de ne pas utiliser ces capacités en cas d'incident, parce qu'elles sont fournies par l'armée. De plus, son infrastructure TIC extensible, sûre, robuste et flexible contribue à la résilience de la Suisse. Elle peut ainsi contribuer de manière déterminante au redémarrage de parties de la société ou d'infrastructures critiques après une cyberattaque étendue.

7.2 Coopération

En complément aux partenariats actuels, qui se focalisent essentiellement sur le RNS, la collaboration avec d'autres services fédéraux et autorités, partenaires économiques et de la société devra être renforcée.

Aujourd'hui déjà, l'armée coopère au quotidien dans le CYBEEM avec différents partenaires, en particulier dans le cadre du RNS. Elle aide dans ce cadre des partenaires du RNS et des tiers à s'acquitter de tâches d'importance nationale, sans devoir eux-mêmes se do-

ter de capacités dans le CYBEEM. Des coopérations existent dans les domaines de l'infrastructure TIC spécialement protégée et des prestations TIC permanentes ou limitées dans le temps. Leur développement, en particulier concernant la mise en réseau des infrastructures et des services TIC, et la mise en place des capacités nécessaires sont en cours de planification et en partie déjà mis en œuvre. Toutes les options y adhèrent. Chaque option poursuit au minimum l'objectif d'améliorer qualitativement les prestations de l'armée au profit de partenaires, en particulier pour ce qui concerne la protection face aux cybermenaces et la capacité de collaborer (interopérabilité) de manière conjointe. L'armée peut également profiter des coopérations, par exemple par l'échange d'informations sur les menaces dans le cyberespace avec d'autres organes fédéraux, des autorités ou des exploitants d'infrastructure critique.

Indépendamment de l'option choisie, d'autres coopérations s'offrent à l'armée, en particulier dans les domaines de l'autoprotection CYBEEM et de la formation. C'est par ailleurs l'échelon politique qui déterminera de quelle manière cela se fera et dans quelle ampleur. S'agissant de l'autoprotection CYBEEM, avec le développement visé, l'armée acquiert la capacité de fournir de manière limitée des prestations de protection au profit de tiers également. Cela vaut, d'une part, pour la surveillance permanente des infrastructures TIC, pour la détection et la neutralisation de cyberattaques et, d'autre part, pour l'appui fourni par des forces spécialisées pouvant intervenir rapidement. Les coopérations peuvent également être étendues dans les domaines de la cryptologie, de la forensique informatique et de la science des données, notamment au DSCC de l'OFS. Dans le cadre de tels exercices et avec l'implication du NCSC, des mécanismes globalement valables et des processus de décision pour la maîtrise des cyberattaques pourraient être développés à l'avenir également.

7.3 Formation

L'armée contribue dans le domaine de la formation à réduire la pénurie de personnel spécialisé, que ce soit à l'aide de la formation donnée dans les stages de l'armée ou dans la formation professionnelle de base des apprentis au sein de l'administration militaire. Avec le stage de formation cyber et l'examen professionnel qui en découle pour devenir un ou une *cyber security specialist*, l'armée s'engage activement et durablement dans le paysage suisse de la formation. Elle entend développer ces coopérations à l'avenir. Grâce à l'instruction préliminaire cyber, elle étend l'offre de formation pour les talents de 16 à 20 ans en Suisse, qui est actuellement plutôt modeste. Les personnes qui suivent cette formation cyber sélective avant le service acquièrent au cours du programme des certificats de capacité qui permettent à des organes externes à l'armée d'identifier le potentiel d'un talent. C'est pourquoi l'armée vise une reconnaissance civile de ces certificats. Les travaux en ce sens avec des partenaires du monde de la formation sont en cours.

Par ailleurs, grâce à la mise en place du *Cyber Training Center*, il existe désormais la possibilité de former des spécialistes sur la base de simulations, qui peuvent faire partie également d'états-majors de crise de partenaires ou de tiers. Dans le cadre de tels exercices et avec l'implication du NCSC, des mécanismes d'une validité générale et des processus de décision pour la maîtrise des cyberattaques pourraient être développés à l'avenir.

En sa qualité d'employeuse, l'armée entend faciliter encore plus l'entrée de talents dans la vie professionnelle, après une formation initiale partiellement ou intégralement accomplie. Elle va ainsi à l'avenir soutenir davantage de travaux de diplôme, par exemple en vue de l'obtention d'un master. Grâce à des stages pour universitaires, elle permet aussi à des personnes talentueuses voulant changer d'orientation professionnelle de démarrer une carrière dans tous les corps de métier ayant trait au CYBEEM. L'armée encourage par ailleurs le perfectionnement spécialisé interne et externe de ses jeunes spécialistes. L'expérience professionnelle acquise par ces jeunes au sein de l'armée est unique en son genre, à la fois du point de vue de son étendue et de ses caractéristiques, et elle est également précieuse dans l'environnement professionnel civil. L'armée considère que l'habituel changement d'orientation professionnelle des spécialistes intégralement formés et possédant quelques années d'expérience professionnelle qui intervient ultérieurement au profit de l'économie ou des autorités civiles est une contribution indirecte à la sécurité de la Suisse.

8

Annexes

8 Annexes

8.1 Annexe 1: composition des lacunes capacitaires à combler

Lacune capacitaire **Autoprotection CYBEEM**	Étape 1	Étape 2	Étape 3
Assurer la protection des systèmes militaires de manière décentralisée		×	× (EEM)
Anticiper l'autoprotection CYBEEM	×		
Déceler et suivre les événements importants pour son autoprotection	×		
Développer des capacités de brouillage radio	×		
Assurer la forensique dans le secteur d'engagement		×	
Supply chain security	×		
Consolider la résilience des infrastructures-clés utilisées dans le cadre de l'autoprotection CYBEEM		×	
Contrôler sa propre image des émissions dans l'espace électromagnétique (EEM)	×		

Tableau 2: lacunes capacitaires en matière d'autoprotection CYBEEM

Lacune capacitaire **Compréhension conjointe de la situation**	Étape 1	Étape 2	Étape 3
Évaluer les quantités de données en recourant à la science des données	(×)	×	
La fusion de toutes les informations relatives à la situation issues de tous les espaces d'opération et de tous les domaines fonctionnels de l'armée et des partenaires permet d'obtenir une compréhension commune de la situation.		×	

Tableau 3: lacunes capacitaires quant à la compréhension commune de la situation

Lacune capacitaire **Traitement robuste et sûr des données**	Étape 1	Étape 2	Étape 3
Datenflüsse degradationsfähig sicherstellen		×	

Tableau 4: lacunes capacitaires dans le traitement sûr et robuste des données

Lacune capacitaire **Conduite en réseau – mesures organisationnelles et techniques**	Étape 1	Étape 2	Étape 3
Assurer l'échange d'informations sans délai entre les systèmes de diverses parties de l'armée		×	
Établir de manière standardisée une image de la situation, en temps opportun et spécifique à l'utilisateur		×	
Associer les partenaires au réseau intégré CRCA		×	

Tableau 5: lacunes capacitaires de la conduite conjointe

Lacune capacitaire **Actions dans l'espace électromagnétique**	Étape 1	Étape 2	Étape 3
Soutenir l'engagement à l'échelon de la conduite tactique		×	×
Développer des effecteurs dans le spectre des fréquences radar			×
Rendre possible une adaptation capacitaire ra-pide et autonome en vue de mener des actions dans l'EEM	×		
Infrastructure-clé SIGINT redondante			×
Capteurs SIGINT/ESM résilients	(×)	×	
SIGINT/ESM aériens	×		
Exploration des systèmes radio à ondes courtes (échelon de la conduite tactique)		×	

Tableau 6: lacunes capacitaires concernant les actions dans l'espace électromagnétique

Lacune capacitaire **Actions dans le cyberespace**	Étape 1	Étape 2	Étape 3
Rendre possible une adaptation capacitaire ra-pide et autonome en vue de mener des actions dans le cyberespace	×		
Soutenir l'engagement jusqu'à l'échelon de la conduite tactique	(×)	×	
Exploration et effet sur les systèmes militaires	(×)	×	

Tableau 7: lacunes capacitaires concernant les actions dans le cyberespace

8.2 Annexe 2: valeurs des axes présentés dans les diagrammes des options au chap. 6

Dimension	Valeur	Description
Autoprotection CYBEEM (qualité)	6	Développer les capacités d'anticiper les menaces et de durer en vue de prévenir les attaques en provenance du CYBEEM (p. ex. cyberattaques)
	7	Complément : surveillance complète des systèmes militaires
	8	Complément : infrastructure-clé résiliente pour l'autoprotection CYBEEM
	9	Complément : capacité à atteindre l'autoprotection CYBEEM autonome et décentralisée à l'aide d'éléments spécialisés
	10	Complément : mise en place spécialisée de capacités en vue de se protéger contre les effets des armes à haute énergie
Autoprotection CYBEEM (quantité)	6	Prestations décentralisées au profit de l'échelon de la conduite opérative
	7	Complément : prestations décentralisées au profit de l'échelon de la conduite tactique (ponctuel)
	8	Complément : prestations décentralisées au profit de l'échelon de la conduite tactique (complet)
	9	Complément : prestations au profit de l'échelon de la conduite de la technique de combat (forces d'intervention, forces médianes et lourdes)
	10	Complément : prestations au profit de l'échelon de la conduite de la technique de combat (autres forces)
Digitalisation (quantité et qualité)	7	Processus numérisés, science des données en tant que service fourni à l'armée, automatisation
	8–10	Non évalués à consignes du document de base conduite de l'action
Effets cyber[130] (qualité)	6	Développement modéré des capacités (qualité)
	7	Développement important des capacités (qualité)
	8–10	Développement jusqu'au plus haut niveau en comparaison avec d'autres forces armées

130 Le présent document étant classifié INTERNE, il n'est pas possible de décrire les cybereffets de manière plus précise. Il en va de même des effets électromagnétiques.

Dimension	Valeur	Description
Profondeur d'engagement cyber (quantité)	6	Effets au profit de l'échelon de la conduite opérative
	7	Complément : effets au profit de l'échelon de la conduite tactique (ponctuel)
	8	Complément : effets au profit de l'échelon de la conduite tactique (complet)
	9	Complément : effets au profit de l'échelon de conduite de la technique de combat (forces d'intervention, forces médianes et lourdes)
	10	Complément : effets au profit de l'échelon de la conduite de la technique de combat (autres forces)
Effets électromagnétiques (qualité)	6	Développement modéré des capacités (qualité)
	7	Développement important des capacités (qualité)
	8	Complément : développement de l'autoprotection de certaines formations et de certains systèmes
	9	Complément : développement de l'autoprotection des forces d'intervention, des forces médianes et lourdes
	10	Complément : développement de l'autoprotection (autres forces)
Profondeur d'engagement électromagnétique (quantité)	6	Effets au profit de l'échelon de la conduite opérative
	7	Complément : effets au profit de l'échelon de la conduite tactique (ponctuel)
	8	Complément : effets au profit de l'échelon de la conduite tactique (complet)
	9	Complément : effets au profit de l'échelon de la conduite de la technique de combat (forces d'intervention, forces médianes et lourdes)
	10	Complément : effets au profit de l'échelon de la conduite de la technique de combat (autres forces)
Réseau (quantité et qualité)	7	Capacité minimale selon les objectifs 2030+ (réseau au sein de l'armée et avec des partenaires externes)
	8–10	Non évalués à consignes du document de base conduite de l'action

8.3 Annexe 3 : liste des abréviations et glossaire

24 / 7	disponibilité 24 heures sur 24 et sept jours sur sept
actif	composant (matériel informatique ou logiciel) d'un environnement informatique
algorithmique	Procédure servant à transformer progressivement des séries de chiffres ; procédure de calcul selon un schéma (répétitif) déterminé Source : https://www.duden.de/rechtschreibung/Algorithmus
AOSS	Autorités et organisations chargées du sauvetage et de la sécurité
APT / advanced persistent threats	Menace pouvant infliger de sérieux dommages à une organisation ou à un pays. L'agresseur est disposé à investir beaucoup de temps, d'argent et de savoir-faire dans ce genre d'attaque ciblée et furtive, et dispose d'importantes ressources. Source : glossaire (admin.ch)
asymétrique	cf. hybride
attaque DDoS	Attaque par déni de service distribué (distributed denial-of-service attack). Il s'agit d'une attaque DoS où la victime est inondée de messages envoyés simultanément par de nombreux systèmes. Source : glossaire (admin.ch)
attribution	détermination de l'origine d'une cyberattaque
augmented reality	réalité augmentée Extension assistée par ordinateur de la perception de la réalité, et pouvant faire appel à tous les sens humains.
BAC	Base d'aide au commandement
big data analysis	Le terme de « big data » désigne des quantités de données qui, par exemple, sont trop grandes, trop complexes, trop volatiles ou trop peu structurées pour pouvoir être évaluées par des méthodes manuelles et conventionnelles de traitement des données.
C2Air	(nouveau) système de surveillance de l'espace aérien et de conduite des opérations aériennes
CdA	chef de l'Armée

CEMA	cyber electromagnetic activities Les CEMA comprennent les opérations dans le cyberespace, la guerre électronique et les opérations de gestion du spectre. Il s'agit d'activités combinées allant au-delà de la zone des effets et qui servent à prendre l'avantage sur l'adversaire tant dans le cyberespace que dans l'espace électromagnétique, à conserver cet avantage et à en tirer profit, tout en empêchant l'adversaire de l'utiliser. Tiré de https://fas.org/irp/doddir/army/fm3-38.pdf (en anglais)
CERT	computer emergency response team / équipe informatique d'urgence
CME	contre-mesures électroniques (electronic counter measures [ECM]) Partie de la guerre électronique qui vise à empêcher l'ennemi d'utiliser l'espace électromagnétique
CNS	communication, navigation, surveillance
COE	Centre des opérations électroniques
combat électronique	Partie de la guerre électronique qui vise à utiliser l'espace électromagnétique ; elle comprend les contre-mesures, les mesures de support et les mesures de protection électronique
COMINT	communication intelligence Exploration de signaux envoyés par ondes électromagnétiques qui servent à communiquer
counter intelligence	contre-espionnage
CTC	Cyber Training Center
CYBEEM	cyberespace et espace électromagnétique
cyber threat intelligence	L'exploration des cybermenaces désigne le fait de collecter des informations sur les menaces et les auteurs de menaces dans le cyberespace et sert à empêcher les cyberattaques.
cyber, cyberespace	Le terme, l'adjectif ou le préfixe cyber, ou son synonyme cybernétique (science constituée par l'ensemble des théories relatives au contrôle et à la régulation), est dérivé du grec kubernan (gouverner). Source : https://www.duden.de/rechtschreibung/cyber_ et le Petit Robert Le terme, l'adjectif ou le préfixe cyber et le cyberespace désignent l'ensemble des infrastructures d'information et de communication (matériel informatique et logiciels) qui échangent des données, les saisissent, les enregistrent, les traitent ou les transforment en action (physiques). Ce terme désigne également les interactions ainsi possibles entre les personnes, organisations et États. Source : Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022
cyberattaque	Acte commis intentionnellement par une personne ou un groupe de personnes dans le cyberespace dans le but de nuire à l'intégrité, la confidentialité ou la disponibilité d'informations ou de données ; selon la nature de l'attaque, celle-ci peut avoir des conséquences sur le plan physique (Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022). Dans le contexte d'une analyse sous l'angle du droit international, il convient de s'intéresser en particulier aux règles du droit international humanitaire et public (Charte de l'ONU).
darknet	Réseau fermé contenant des sites web qui ne sont pas indexés dans des moteurs de recherche normaux et que l'on trouve via le navigateur Tor. Les navigateurs Tor permettent de se déplacer sur Internet ou le darknet en restant anonyme.
DDPS	Département fédéral de la défense, de la protection de la population et des sports
dégradable	Par dégradation, on entend la séparation des composants des réseaux informatiques. La fonctionnalité des composants séparés est entièrement maintenue.
DEVA	développement de l'armée
DFF	Département fédéral des finances
EEI	engins explosifs improvisés (improvised explosive device [IED])
EEM	espace électromagnétique
EPM	electronic protective measures (mesures de protection électronique)
ESM	electronic support measures (mesures de support électronique)
EW	electronic warfare (guerre électronique)
exploration électronique	Partie de l'exploration des signaux qui vise à collecter des informations en enregistrant et évaluant les ondes électromagnétiques de systèmes étrangers de repérage et de guidage
exploration électronique des signaux (SIGINT)	Partie de la guerre électronique qui vise à collecter des informations en enregistrant et évaluant les signaux électromagnétiques étrangers. Elle comprend l'exploration électronique et l'exploration radio.

explorer	Recherche active, dans un domaine ou un espace de recherche d'informations déterminé, d'informations concernant un adversaire, la partie adverse ou d'autres acteurs
fédération	regroupement d'organisations, de domaines ou d'États
FITANIA	Programme permettant à l'armée et aux organisations de sécurité civiles de disposer de systèmes TIC capables de relever les défis futurs L'abréviation FITANIA signifie en allemand Führungsinfrastruktur, Informationstechnologie und Anbindung an die Netzinfrastruktur der Armee, soit « infrastructure de conduite, technologie de l'information et liaison avec l'infrastructure de réseau de l'armée ».
FMN	Le Federated Mission Networking (réseau de conduite d'opérations en coalition) vise à garantir l'interopérabilité et la capacité de commandement en améliorant l'échange d'informations entre les partenaires et les systèmes.
forensique dans le secteur d'engagement / forensique informatique	Mise en sûreté et évaluation des moyens de preuve afin de constater ce qui s'est passé sur un appareil
friendly force tracking	Un friendly force tracking (suivi des forces amies) efficace fournit à plusieurs niveaux l'emplacement des propres forces armées et des éventuelles troupes de la coalition dans la zone d'engagement.
GE	guerre électronique
GEC	gestion de l'engagement et de la carrière
honeypot	Le terme honeypot (pot de miel) désigne, en jargon informatique, un programme ou un serveur simulant un ordinateur, un réseau complet ou le comportement d'utilisateurs fictifs. Les pots de miel servent à observer le comportement et à enregistrer les méthodes d'attaque des pirates. Source : glossaire (admin.ch)
hybride	composé de plusieurs éléments Source : https://www.duden.de/rechtschreibung/Hybrid La menace hybride, soit le combat hybride, est l'expression employée pour désigner une composition flexible des moyens réguliers, irréguliers, symétriques, asymétriques, militaires et non-militaires utilisés de manière ouverte et clandestine lors d'un conflit. Ces moyens visent à atténuer la différence entre les états binaires existant dans le droit international que sont la guerre et la paix. Source : Avenir des forces terrestres (admin.ch)
IA	intelligence artificielle (artificial intelligence [AI])
IC	infrastructures critiques Par infrastructures critiques, on entend les processus, systèmes et installations indispensables au fonctionnement de l'économie et au bien-être de la population.
LAAM	loi sur l'armée
MDO	multi domain operation, opération militaire couvrant l'ensemble du spectre des espaces d'opération
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
mesures de support électroniques	Partie du combat électronique qui vise à explorer les buts et les effets et à identifier les menaces dans l'espace électromagnétique
mil	militaire
MOTS	merchandise off the shelf / matériel informatique standard
MRO	maintenance repair operations / maintenance, réparation, exploitation
nuage	collection virtuelle de ressources informatiques
numérisation (ou digitalisation)	La numérisation [ou digitalisation] est la conversion d'un signal (vidéo, image, audio, caractère d'imprimerie, impulsion, etc.) en une suite de nombres permettant de représenter cet objet en informatique ou en électronique numérique (glossaire de l'OFCOM : Stratégie Suisse numérique)
OFCOM	Office fédéral de la communication
opération d'information	Par opération d'information, on entend un type d'engagements des forces armées exerçant une influence sur les informations de l'ennemi et protégeant ses propres informations et systèmes d'information.
OTAN	Organisation du traité de l'Atlantique nord
PACD	Plan d'action Cyberdéfense DDPS
patriotic hackers	personnes agissant au profit d'un État, temporairement ou sur la base d'un mandat
procédure reach-back	L'effecteur se trouve dans la zone d'engagement, l'effet de l'arme est déclenché à distance.

réseau de zombies	Réseau d'ordinateurs infectés par des programmes malveillants (bots). Un pirate (le propriétaire du réseau de zombies) les contrôle complètement à distance. Un réseau de zombies peut compter de quelques centaines à des millions d'ordinateurs compromis. Source : glossaire (admin.ch)
réseau intégré CRCA	Réseau intégré de capteurs, de renseignement, de conduite et d'action
résilience	Aptitude d'un système, d'une organisation ou d'une société à résister à des perturbations et à conserver sa capacité de fonctionnement ou à la retrouver aussi rapidement que possible (Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022)
reverse engineering	rétro-ingénierie, ingénierie inverse ou inversée Activité qui consiste à étudier un objet pour en déterminer le fonctionnement interne, la méthode de fabrication et peut-être dans l'intérêt de le modifier
RNS	Réseau national de sécurité
RSO	radar à synthèse d'ouverture (synthetic aperture radar [SAR])
science des données	La science des données est un domaine d'application interdisciplinaire permettant d'établir des méthodes et des processus d'extraction de modèles et d'informations à partir de quantités de données importantes, trop complexes, trop volatiles ou trop peu structurées. Pour ce faire, on utilise des techniques et méthodes d'automatisation du comportement intelligent et de l'apprentissage machine.
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
Stuxnet	Stuxnet est un ver informatique ciblant à l'origine les installations nucléaires iraniennes. Après avoir muté, il s'est ensuite propagé à d'autres installations électriques ou industrielles. Source : https://www.mcafee.com/enterprise/de-de/security-awareness/ransomware/what-is-stuxnet.html
supply chain security	Sécurité de la chaîne d'approvisionnement ou sécurité de la chaîne de valeur ajoutée
système de cryptage	Technique ayant pour but de chiffrer un message, c.-à-d. de le rendre inintelligible pour ceux à qui il n'est pas destiné. La cryptographie permet d'assurer la sécurité des transactions et la confidentialité des messages. Glossaire (admin.ch)
systèmes TIC	systèmes dans lesquels les TIC sont utilisées et mises en œuvre techniquement
technologie de blockchain	Une blockchain (ou chaîne de blocs) est une liste de données perpétuellement extensible, ces données étant regroupées en blocs reliés au moyen de procédures cryptographiques. Chaque bloc contient habituellement un hachage sûr cryptographié du bloc précédent, un horodatage et les données de la transaction.
technologies immersives	Les technologies immersives permettent aux mondes physique et numérique de se fondre. Soit elles représentent entièrement la réalité virtuellement (réalité virtuelle), soit elles enrichissent l'environnement d'informations numériques (réalité augmentée).
TI	technologies de l'information, informatique
TIC	technologies de l'information et de la communication
wargaming	Ces dernières années, le wargaming est toujours plus utilisé dans le contexte de la planification d'actions visant à vérifier les variantes et en particulier à prendre des décisions.

8.4 Annexe 4 : bibliographie

Internet

Abschlussbericht Aufbaustab Cyber- und Informationsraum 2016. Ministère fédéral de la défense (DE) 2016.
http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf

Gaycken Sandro, Talbot, David : Aufmarsch im Internet, in : Technology Review, 08.10.2010. https://m.heise.de/tr/artikel/Aufmarsch-im-Internet-1102301.html

Gilbert David : A bunch of kids probably pulled off the biggest DDoS hack ever, in : Vice News, 04.11.2016.
https://www.vice.com/en_us/article/3k58e5/a-bunch-of-kids-probably-pulled-off-the-biggest-ddos-hack-ever

Kamasa Julian : Pour une politique de sécurité transparente, Avenir Suisse, 17.06.2019.
https://www.avenir-suisse.ch/fr/de-la-necessite-dune-politique-de-securite-transparente/

MacKenzie Paul : Cyberspace and Cyber-Enabled Information Warfare, in : Joint Air Power Competence Centre, 2018.
https://www.japcc.org/cyberspace-and-cyber-enabled-information-warfare/

Patalong Frank : Untersee-Kabel : Die fragilen Lebensadern des Internets, in : Der Spiegel, 02.02.2015.
https://www.spiegel.de/netzwelt/web/untersee-kabel-die-fragilen-lebensadern-des-internets-a-1015809.html

Ruhmann Ingo : Aufrüstung im Cyberspace. Staatliche Hacker und zivile IT-Sicherheit im Ungleichgewicht, in : Wissenschaft & Frieden, dossier 79, 3e éd., 2015.
https://wissenschaft-und-frieden.de/seite.php?dossierID=083

Sicherheitslücken im Internet, C.I.A. Prinzip, Universität Oldenburg (DE), 2020.
http://www.informatik.uni-oldenburg.de/~iug10/sli/index.html

Simonite Tom : NSA's Own Hardware Backdoors May Still Be a "Problem from Hell", in : MIT Technology Review, 08.10.2013.
https://www.technologyreview.com/2013/10/08/176195/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/

Forces armées allemandes :
https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum

Forces armées finlandaises :
https://puolustusvoimat.fi/en/about-us/c5-agency

Forces armées françaises :
Direction générale de l'armement (defense.gouv.fr)

Forces armées britanniques :
https://www.theguardian.com/technology/2020/feb/27/uk-to-launch-specialist-cyber-force-able-to-target-terror-groups ;
https://www.independent.co.uk/news/uk/home-news/cyber-warfare-security-force-iran-crisis-ministry-of-defence-a9278591.html

Forces armées néerlandaises :
https://english.defensie.nl/topics/cyber-security/cyber-command

Publications

Plan d'action Cyberdéfense DDPS (PACD), Département fédéral de la défense, de la protection de la population et des sports (DDPS) (éd.), Berne 2017.
Aktionsplan für Cyber-Defence APCD (admin.ch)

Baezner Marie, Cordey Sean : Nationale Cybersicherheitsstrategien im Vergleich – Herausforderung für die Schweiz, mars 2019, Center for Security Studies (CSS), EPFZ 2019.
Risk and Resilience Reports – Center for Security Studies | EPFZ

Baezner Marie, Robin Patrice : Hotspot Analysis : Stuxnet, October 2017, Center for Security Studies (CSS), EPFZ 2017.
Risk and Resilience Reports – Center for Security Studies | EPFZ

La politique de sécurité de la Suisse. Rapport du Conseil fédéral (16.061), 24.08.2016, FF 2016 7549.
La politique de sécurité de la Suisse. Rapport du Conseil fédéral (admin.ch)

Lutter plus efficacement contre le terrorisme et le crime organisé. Rapport du Conseil fédéral donnant suite au postulat du 21 février 2005 de la Commission de la politique de sécurité du Conseil des États (05.3006), 09.06.2006, FF 2006 5421.
FF 2006 5421 (admin.ch)

Système d'interception des communications par satellites du Département fédéral de la défense, de la protection de la population et des sports (projet « Onyx »). Rapport de la Délégation des commissions de gestion des Chambres fédérales du 10.11.2003.
Système d'interception des communications par satellites du Département fédéral de la défense, de la protection de la population et des sports (projet « Onyx »). Rapport de la Délégation des commissions de gestion des Chambres fédérales du 10.11.2003 (parlament.ch)

Avenir de la défense aérienne. Sécurité de l'espace aérien pour la protection de la Suisse et de sa population. Rapport du groupe d'experts Prochain avion de combat, Département fédéral de la défense, de la protection de la population et des sports (DDPS) (éd.), Berne 2017.
Avenir de la défense aérienne. Sécurité de l'espace aérien pour la protection de la Suisse et de sa population. Rapport du groupe d'experts Prochain avion de combat

Avenir des forces terrestres. Rapport sur les perspectives de développement des capacités des forces terrestres, Département fédéral de la défense, de la protection de la population et des sports (DDPS) (éd.), deuxième version révisée, Berne 2019.
Avenir des forces terrestres (admin.ch)

Message du 19 février 2014 concernant la loi sur le renseignement, FF 2014 2029.
Message concernant la loi sur le renseignement (admin.ch)

Message du 3 septembre 2014 relatif à la modification des bases légales concernant le développement de l'armée, FF 2014 6693.
FF 2014 6693 (admin.ch)

Message du 29 janvier 2020 sur le programme de la législature 2019 à 2023 (19.078), FF 2020 1709.
Message sur le programme de la législature 2019 à 2023 (admin.ch)

Coats Daniel : Worldwide Threat Assessment of the US Intelligence Community, 13.02.2018.
https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Cordey Sean, Dewar Robert S., ed. : National Cybersecurity and Cyberdefense Policy Snapshots : Update Collection 2, 2019, Center for Security Studies (CSS), EPFZ 2019.
Risk and Resilience Reports – Center for Security Studies | EPFZ

Cordey Sean : Cyber Influence Operations : An Overview and Comparative Analysis, Cyber Defence Trend Analysis, Center for Security Studies, EPFZ 2019.
Risk and Resilience Reports – Center for Security Studies | EPFZ

Cyber and Electromagnetic Activities : Joint Doctrine Note 1/18, Development, Concepts and Doctrine Centre, UK Ministry of Defence, Swindon (UK) 2018.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf

Cyber Electromagnetic Activities : Field Manual FM 3.38, Headquarters Department of the Army, Washington D.C.(US) 2014.
https://fas.org/irp/doddir/army/fm3-38.pdf

Dewar Robert S. : Trend Analysis : Contextualising Cyber Operations, mai 2018, Center for Security Studies (CSS), EPFZ 2019.
Risk and Resilience Reports – Center for Security Studies | EPFZ

Digitaler Stillstand, Die Verletzlichkeit der digital vernetzten Gesellschaft, Académie autrichienne des sciences 2017.
http://epub.oeaw.ac.at/0xc1aa5576_0x00358488.pdf

Evan Tamara : Cyber Terrorism Threat Intelligence and Loss Modelling, in : Cambridge Centre for Risk Studies 2018, Risk Summit 2018.
https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/180620-slides-evan.pdf

Gaycken, Sandro : Einführung Cyberwar : Was ist Cyberwar. 2013
https://www.inf.fu-berlin.de/groups/ag-si/pub/Cyberwar_SB1-5_V160114.pdf

Schörnig Niklas : Resilienz stärken und Vertrauen bilden statt den Cyberwar herbeireden, in : Werkner Ines-Jaqueline / Schörnig Niklas : Cyberwar – die Digitalisierung der Kriegsführung : Fragen zur Gewalt, vol. 6, Wiesbaden (DE) 2019.

Schulze Sven-Hendrick : Cyber-»War» – Testfall der Staatenverantwortlichkeit, Tübingen (DE) 2015.

Schürz Torben : Der vernetzte Krieg. Warum moderne Streitkräfte von elektronischer Kampfführung abhängen, in : DGAPkompakt 17, 16.10.2015.
https://dgap.org/system/files/article_pdfs/2019-17-DGAPkompakt.pdf

Segal Adam : The Hacked World Order, New York, United States Public Affairs, 2016

Sigholm Johan : Non-State Actors in Cyberspace Operations, in : Journal of Military Studies, vol. 4, 2013.

Slayton Rebecca : What Is the Cyber Offense-Defense Balance ? Conceptions, Causes, and Assessment, in : International Security ; The MIT Press, vol. 41, 3e éd., Cambridge (US) 2017.

Smeets Max : The Strategic Promise of Offensive Cyber Operations, in : Strategic Studies Quarterly, vol. 12, 22.09.2018.
https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Smeets.pdf

Stratégie Suisse numérique, Office fédéral de la communication (OFCOM), Bienne 2020.
Numérisation (admin.ch)

Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022, Unité de pilotage informatique de la Confédération (UPIC) (éd.), Berne 2018.
Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018-2022 (admin.ch)

Swisscom Cyber Security Report 2019 : L'attaque ciblée.
https ://documents.swisscom.com/product/filestore/lib/c09ea7dd-a677-4d3a-883d-303240d36b8f/Swisscom_Security_Report_2019_FR.pdf

The Global Disinformation Order : Global Inventory of Organized Social Media Manipulation ; University of Oxford (UK) 2019.
https ://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Impressum

Editeur	Département fédéral de la défense, de la protection de la population et des sports (DDPS)
Rédaction	Groupe d'experts conception générale cyber
Premedia	Centre des médias numériques de l'armée (MNA), 86.084 d
Copyright	02.2022, VBS
Internet	www.armee.ch