Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

09.11.2017

PLAN D'ACTION CYBERDEFENSE DDPS (PACD)

PLAN D'ACTION CYBERDEFENSE DDPS (PACD)

AVANT-PROPOS

Le *Plan d'Action Cyberdéfense du DDPS* (PACD) est un développement interne au DDPS. Son élaboration a débuté en juillet 2016 par un état des lieux puis la définition d'une stratégie. Approuvées en octobre 2016, ces étapes ont été suivies d'un plan de mise en œuvre adopté à son tour en juin 2017.

La publication de ce plan d'action intervient suite à une demande déposée conformément à la Loi sur la transparence. Ce plan d'action étant composé de documents techniques avec de nombreux éléments classifiés, la mise à la disposition du public de versions partiellement masquées l'aurait rendu grandement incompréhensible. Le DDPS souhaitant cependant qu'il soit autant que possible accessible, a privilégié la mise à disposition d'un document unique et simplifié. Lorsque cela est pertinent, en plus du contenu original des documents de base, le présent document tient aussi compte de l'actualité.

Cette documentation est disponible sur Internet
http://www.vbs.admin.ch/fr/defense/protection-cyberattaques.html

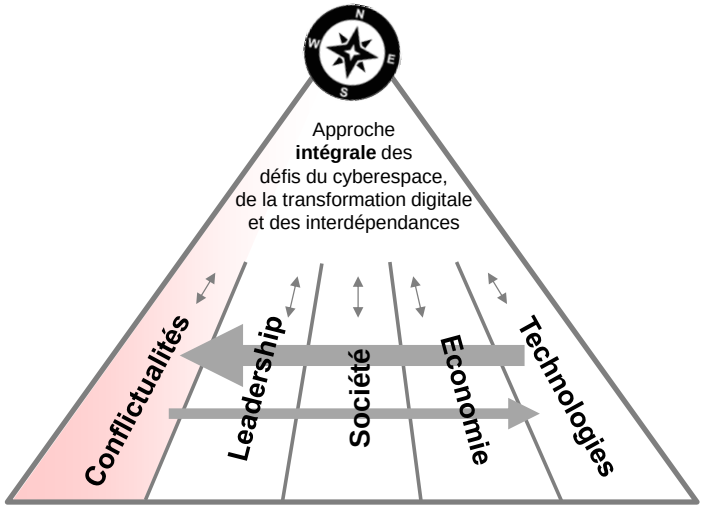
Abréviations

CERT	Computer Emergency Response Team
ISMS	Information Security Management System (selon ISO 27000)
ENISA	European Network and Information Security Agency
LMS	Learning Management System
MELANI	Melde- und Analysestelle Informationssicherung
OIC	Operation Information Center
PACD	Plan d'Action Cyberdéfense DDPS
RAPOLSEC	Rapport du Conseil fédéral sur la politique de sécurité de la Suisse
SIO	Sécurité des informations et des objets (la SIO est une division du Secrétariat général du DDPS)
SNPC	Stratégie nationale pour la protection de la Suisse contre les cyberrisques
SRC	Service de renseignement de la Confédération
TIC	Technologies de l'information et de la communication

RESUME

Les défis du cyberespace pour la politique de sécurité

Le développement technologique et la numérisation des activités humaines ont donné naissance au cyberespace dont notre société est irrémédiablement dépendante et qui vit une transformation en profondeur de ses modes de fonctionnement. Cette évolution comporte de très nombreux points positifs, mais engendre aussi de nouveaux risques et de nouvelles formes de conflictualités qui se renouvellent sans cesse. La nature même des conflits s'en trouve bouleversée.



Les cyberattaques ne sont plus des perturbations mineures aux effets peu tangibles, de portée et de durée limitées, provoquées par des vandales ou des criminels ne disposant que de faibles moyens; elles résultent désormais d'une chaîne causale complexe et sont le fait d'une diversité inédite d'acteurs privés et étatiques toujours plus professionnels, aux multiples motivations et agissant dès le temps de paix en abusant de l'environnement civil. Les conséquences sont importantes et même si la Suisse n'a jusqu'ici pas à déplorer d'effets à grande échelle, l'évolution des défis du cyberespace doit nous alerter et une **approche intégrale** s'impose pour l'appréhender. C'est un défi majeur pour notre politique de sécurité.

Mission du DDPS dans le cyberespace et état de ses moyens

Avec le développement du cyberespace et conformément à la Stratégie Nationale pour la protection de la Suisse contre les cyberrisques (SNPC, en cours de révision sous la direction du Département fédéral des finances), le DDPS doit assurer la défense de ses propres systèmes et infrastructures afin d'être en tout temps et toute circonstance en mesure de remplir ses missions, y.c. l'assistance des opérateurs d'infrastructures critiques en cas de cyberattaque.

Les moyens et procédures du DDPS ne sont cependant pas à la hauteur des défis posés par le cyberespace, en particulier en cas d'augmentation du nombre et de la complexité des incidents. Les possibilités de porter assistance aux opérateurs d'infrastructures critiques subissant des cyberattaques s'en trouvent en conséquence significativement affectées.

Les enseignements tirés de la cyberattaque contre RUAG en 2016 ont montré qu'il manquait également au DDPS un élément de conduite stratégique pour analyser de manière intégrale et comprendre à temps les défis de la transformation digitale. Pour combler ces lacunes, le chef DDPS a ordonné en 2016 l'élaboration du PACD dont les premiers résultats concrets sont déjà visibles.

Stratégie du DDPS et contenu du plan d'action

Le Plan d'action cyberdéfense a été réalisé dans le cadre des moyens et compétences propres au DDPS. Il a été développé dans l'esprit de la SNPC et ne préjudicie pas son prochain développement et leur coordination est en cours. De fait, une fois réalisé, ce plan d'action constituera un renforcement essentiel du dispositif de défense de la Suisse face aux cybermenaces.

Pour établir le Plan d'action cyberdéfense, le chef DDPS a formulé le résultat à atteindre comme suit:

En étroite collaboration avec ses partenaires, l'économie et les hautes écoles, le DDPS entend être un pôle de compétence reconnu en matière de cyberdéfense, capable avec des moyens suffisants, en quantité et qualité, d'atteindre les buts suivants:

- affronter, en tant qu'infrastructure critique et dans le cadre de ses compétences, l'augmentation continue en quantité, intensité et complexité des différentes formes de cyberconflictualités, au quotidien déjà et en cas de crise et de conflit ;
- mettre concrètement en œuvre les aspects cyber de la Loi sur le renseignement (LRens) et de la Loi militaire (LAAM);
- assister efficacement et durablement les opérateurs d'infrastructures critiques subissant des cyberattaques.

Le Plan d'action cyberdéfense précise les **prestations** du DDPS, notamment l'engagement subsidiaire des moyens de l'armée au profit des autorités civiles et détaille les **processus** pour assurer un engagement optimal des moyens. Il est un ensemble cohérent basé sur une **architecture** qui organise logiquement les fonctions composant la cyberdéfense. Les défis et crises relatifs au cyberespace étant par nature complexes et inter-domaines, ce plan établit une gouvernance forte et énumère les **capacités** requises, à savoir la conduite, l'anticipation, la protection, la prévention, la réaction, l'action et l'assistance aux autorités civiles.

Réalisation du Plan d'action cyberdéfense

Le Plan d'action cyberdéfense n'entraîne pas de révolution, d'autant que de nombreuses mesures ont déjà été prises. Il vise à **optimiser** et à **renforcer** les moyens du DDPS afin de lui permettre d'agir avec succès dans le cyberespace, aussi en cas de crise majeure.

Trois efforts principaux sont prévus qui, en raison de la rapide évolution des défis du cyberespace, seront continuellement adaptés. Il s'agit premièrement de la **gouvernance** pour assurer la conduite stratégique du domaine. Vient ensuite le développement des **moyens opérationnels** qui fera passer l'effectif actuel d'env. 50 à 150 collaborateurs d'ici à 2020 au moyen d'une réallocation interne des moyens du DDPS, et ce malgré les économies ordonnées. Enfin il s'agit des **renforts** apportés au noyau professionnel par les militaires de milice, ainsi qu'une forte collaboration du DDPS avec ses partenaires au sein d'un *CYD-Campus* qui, selon les ambitions du DDPS, devrait produire ses premiers effets en matière de prospective, de mutualisation des moyens et d'instruction dès 2018 déjà. Le défi central du Plan d'action cyberdéfense sera de trouver les postes et talents nécessaires. Selon les premières estimations, cet effort coûtera annuellement au DDPS environ 2% de ses ressources.

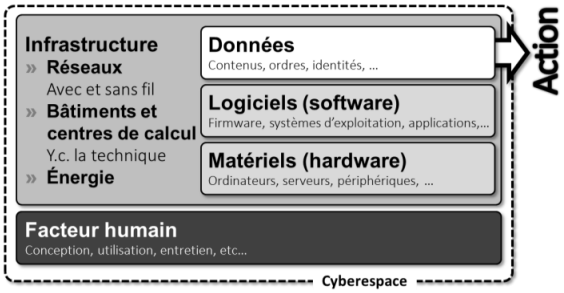
Un premier pas impératif

La défense de la Suisse doit s'adapter aux défis innombrables de la transformation numérique de la société. En raison de la rapidité de l'évolution de ce domaine, le développement de nos capacités de cyberdéfense ne peut pas attendre. L'absence d'attaques majeures jusqu'ici ne saurait être une excuse pour retarder notre effort, car les acteurs mal intentionnés profitent déjà de nos lacunes et pourraient, en cas de conflit nous infliger des dégâts insupportables. Le Plan d'action cyberdéfense n'est cependant ni une assurance absolue ni un aboutissement; il est la feuille de route initiale du DDPS pour lui permettre de s'adapter en continu aux défis d'un cyberespace devenu un **enjeu majeur de notre politique de sécurité.**

TABLE DES MATIERES

1 EXPOSÉ DE SITUATION

1.1 Le cyberespace



Le terme de *cyberespace* désigne l'environnement dans lequel les données sont acquises, sauvegardées, utilisées et transmises, créant ainsi également des effets physiques. Ce terme englobe cependant bien plus que l'informatique car celle-ci nécessite impérativement de l'énergie électrique, des infrastructures et aussi des personnes à tous ses stades de développement. Cet espace évolue très vite, révolutionnant tant notre manière de vivre que la nature des conflits. Il est la clé de multiples progrès mais également de vulnérabilités critiques. Ses principales caractéristiques sont la complexité, les interdépendances, la quasi disparition des limites temporelles et géographiques, l'anonymat et donc la difficulté d'attribuer précisément des actions à des acteurs.

1.2 Dangers et menaces dans le cyberespace

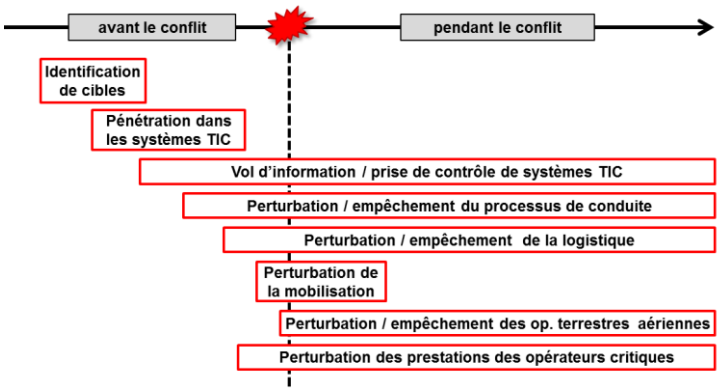
L'État, l'économie et la société reposent de plus en plus sur les réseaux digitaux mondialisés. Ils deviennent ainsi dépendants et vulnérables face à des atteintes à leur disponibilité, intégrité et confidentialité. Les possibilités d'abuser de ces vulnérabilités à des fins personnelles, criminelles, terroristes et étatiques (actions militaires et/ou de renseignement) deviennent pratiquement illimitées. Défendre le cyberespace revient alors à comprendre et à composer avec des acteurs hétérogènes, tant en matière de compétences que de ressources, la palette allant de l'amateur isolé à la grande puissance disposant de moyens quasi illimités en passant par des réseaux criminels toujours plus agiles et innovants.

Dans le cadre de ses tâches originaires, le DDPS distingue 4 domaines:

- **La lutte contre le renseignement prohibé**: le cyberespionnage gagne en importance dans les services du monde entier; les actions via le cyberespace permettent non seulement d'appuyer les méthodes d'espionnage classiques qui ne disparaissent pas, mais aussi d'offrir de nouvelles options à des coûts comparativement faibles et une prise de risque limitée; du fait de la variété d'acteurs présents, les attaques peu sophistiquées réalisées avec des outils librement disponibles sur Internet et relativement aisées à combattre, côtoient des outils hautement complexes et difficiles à déceler.
- **La lutte contre le terrorisme:** les groupes terroristes maîtrisent l'usage des médias sociaux pour leur communication et parviennent à toucher un large public; le cyberespace représente pour eux un vecteur clé pour leur financement, recrutement, formation et propagande; Internet leur offre toujours plus de possibilités offensives et bien que leurs actions n'aient entraîné jusqu'ici que des conséquences limitées, il faut s'attendre à ce qu'ils disposent tôt ou tard de la capacité à réaliser des actions sophistiquées et destructrices.
- **La protection des infrastructures critiques:** les opérateurs d'infrastructures critiques sont confrontés à toute la gamme des cybermenaces, que ce soit le cyberespionnage, le cybersabotage ou la cybercriminalité; des cyberattaques dirigées contre ces infrastructures peuvent affecter des fonctions vitales pour la société, provoquer des conséquences particulièrement lourdes ainsi que des réactions en chaîne insoupçonnées; comme le démontre chaque panne, l'énergie électrique dont dépendent le cyberespace, les télécommunications, les services financiers, la logistique ou encore le système de santé et la sécurité, est un des éléments particulièrement critiques.

- **La défense militaire:** le cyberespace devient un *terrain d'opérations* militaires à part entière et un nombre croissant de pays se préparent à y combattre; cette évolution nécessite une adaptation comparable à celle d'il y a environ 100 ans lorsque la guerre gagnait le ciel. Dans le cyberespace, comme dans les airs, il ne s'agit cependant pas de se préparer uniquement pour la guerre, mais d'assurer en permanence la disponibilité, l'intégrité et la confidentialité des fonctions dont nous sommes dépendants. La logique réactive et ponctuelle actuellement dominante doit faire place à une logique d'anticipation et de résilience afin de pouvoir répondre à des événements simultanés et massifs.

Les cyberattaques de 2015 et 2016 contre des infrastructures critiques ukrainiennes montrent que dans un conflit moderne, les infrastructures critiques se retrouvent parmi les premières cibles. Au sein d'une société comme la nôtre, dépendante de ces infrastructures, l'effet de levier est particulièrement important. Il y a donc lieu de leur assurer la meilleure protection et défense possible, surtout dans le domaine de l'énergie électrique. Des cyberattaques contre le DDPS et l'armée ou contre les prestataires dont ils dépendent auraient un impact immédiat sur leur disponibilité à l'engagement et donc sur les opérations. Un tel impact peut aller du léger dérangement au blocage complet de tout ou partie des moyens. Comme suggéré dans la figure ci-contre, la défense durant la phase avant le conflit est essentielle.



1.3 Evolution des cybermenaces

Selon le *World Economic Forum*, les conséquences mondiales annuelles de la cybercriminalité pour l'économie avoisinent les 450 milliards US$, soit 0.82% du PIB mondial et la tendance est clairement à la hausse, même s'il reste difficile d'articuler des chiffres précis. L'observation montre par ailleurs que les agressions – tant étatiques que du fait d'acteurs privés – se multiplient. Comme constaté dans les conflits autour de l'Ukraine et de la Syrie notamment, la situation géopolitique actuelle contribue à un usage toujours plus agressif du cyberespace. Il faut s'attendre à des actions malveillantes devenant toujours plus sophistiquées, massives et durables. Grâce à la vitesse et à l'anonymat qui les caractérisent, ces actions occuperont une place toujours plus grande dans les conflits armés, y.c. en matière d'influence, bien avant l'usage d'armes classiques.

Le nombre d'applications et de systèmes connectés à Internet (Internet des objets) croît fortement, ainsi que le transfert des données dans des *clouds*. La sécurité de ces objets est non seulement faible, mais en plus les utilisateurs ne parviennent plus à déterminer ni à contrôler les fonctions qui s'exécutent sur leurs machines ni par exemple les chemins employés par les contenus informationnels. La perte de contrôle quant aux processus et données sensibles est inexorable. Les secteurs privés et publics, sous pression pour économiser, optimiser ou encore offrir davantage de confort ou de fonctionnalités, alimentent eux-mêmes les développements et comportements mettant leurs activités en danger.

Aux éléments évoqués ci-dessus il faut ajouter la nécessaire prise en compte de l'émergence incessante et rapide de nouvelles technologies et des usages – positifs comme négatifs – qui pourraient en être faits et qui doivent donc être accompagnées par une réflexion intégrale continue.

1.4 Tâches et bases légales du DDPS

En raison de sa nature transversale, le cyberespace dépasse le cadre du DDPS. Néanmoins, afin d'éviter toute fausse interprétation ou attente, le tableau qui suit précise ses tâches. Dans une approche anticipative, ce tableau tient compte, là où un consensus se détache clairement, des éléments de la Loi sur la sécurité de l'information (LSI) en cours de développement et de la Stratégie de protection de la Suisse contre les cyberrisque (SNPC) en cours de révision sous la conduite du Département fédéral des finances.

	Cyberprotection[1]	**Cyberdéfense**	**Action dans le cyberespace**
Pour le citoyen / individu	Chacun est responsable de sa propre protection.	En cas d'incident, intervention de la chaine de poursuite pénale.	Non applicable
Pour l'économie	Chaque entreprise est responsable de sa protection. Des normes particulières peuvent être édictées par les branches ou diverses autorités.	Chaque entreprise est responsable de sa défense. En cas d'incident, intervention de la chaine de poursuite pénale. Appui du DDPS possible (décision politique) en cas de haute criticité.	
Pour les infrastructures critiques	Chaque opérateur d'infrastructure critique est responsable de sa protection. Des normes particulières peuvent être édictées par les branches ou diverses autorités. Des collaborations en matière de prévention avec le SRC et l'armée sont établies.	Chaque opérateur d'infrastructure critique est responsable de sa défense. Le SRC peut prêter assistance en cas de cyberattaque (au besoin avec des contre-mesures offensives). Si les conditions sont remplies, l'armée peut (subsidiairement) l'appuyer.	
Pour le DDPS	Le DDPS est responsable de sa propre protection. Il applique les normes de la Confédération et celles propres à ses besoins spécifiques.	Le DDPS est responsable de sa propre défense (au besoin avec des contre-mesures offensives).	Le DDPS produit les effets requis par la réalisation des tâches originaires de ses offices et de l'Armée.

En 2009, l'avis de droit de la Direction du Droit international public (DFAE) et de l'Office fédéral de la justice (DFJP) montrait que les bases légales ne suffisaient que pour des activités passives de défense. La Loi sur le renseignement approuvée en votation populaire en septembre 2016 et la Loi sur l'armée approuvée par le Parlement en mars 2016 comblent les lacunes relevées par cet avis de droit en matière de défense active. Le cadre clarifié pour le DDPS est résumé ci-après.

Armée		Situation normale (service d'instruction, service d'assistance)[2]
Cyberprotection		autorisé
Cyberdéfense	passif	
	actif	soumis à autorisation en cas de cyberattaque contre l'armée (art. 100 al. 1 lit. c LAAM)
Action dans le cyberespace	passif	autorisé
	actif	non autorisé

[1] Définitions de travail: *Cyberprotection*: ensemble des mesures visant à protéger les systèmes et infrastructures TIC contre les cyberrisques et à assurer leur résilience. *Cyberdéfense*: ensemble des mesures visant à détecter et identifier les menaces et attaques visant les systèmes et infrastructures TIC et à y répondre, au besoin par des contremesures offensives. *Actions dans le cyberespace*: ensemble des mesures prises contre un adversaire dans le cyberespace pour acquérir des renseignements ou porter atteinte à la disponibilité ou à l'intégrité de ses systèmes ou infrastructures TIC.

[2] En service actif s'ajoutent les règles du Droit international humanitaire.

Service de renseignement de la Confédération		En toute situation
Cyberprotection		autorisé
Cyberdéfense	passif	
	actif	soumis à autorisation en cas de cyberattaque contre des infrastructures critiques (Art. 26 al. 1 lit. d chiffre 2 LRens; Art. 37 al. 1 LRens)
Action dans le cyberespace (que l'exploration)	passif	autorisé
	actif	soumis à autorisation (en Suisse, selon art. 26, lit. d)

1.5 Moyens en personnel du DDPS

En matière de cybersécurité, la question des moyens en personnel est souvent au premier plan des intérêts. En réponse à l'interpellation 17.3103[3], le Conseil fédéral a rendu public les détails suivants: […] *ressources dans le cadre de la Stratégie nationale pour la protection de la Suisse contre les cyberrisques. Elle dispose à cet effet d'environ 86 postes (50 au DDPS, 20 au DFJP, 10 au DFF, 2 au DFAE, 2 au DEFR et 2 au DETEC), dont 30 étaient à durée déterminée avant d'être confirmés le 26 avril 2017 par le Conseil fédéral. Ces postes permettent de traiter les incidents quotidiens. L'augmentation de l'intensité et des conséquences des cybermenaces décrites dans le Rapport de politique de sécurité 2016 impose toutefois un réexamen qui est prévu dans le cadre de la révision de la SNPC. Dans le cadre de son Plan d'Action Cyberdéfense, le DDPS a d'ores et déjà indiqué son intention d'augmenter significativement ses effectifs d'ici à 2020.*

Il est cependant erroné de se focaliser uniquement sur le nombre de postes dédiés. Les outils techniques, les processus, le réseau des personnes, la confiance, la qualité de l'échange d'information, la plus-value apportée par la milice, doivent tout autant être considérés pour évaluer la force d'un dispositif. En l'état cependant, et bien que le DDPS dispose d'un personnel professionnel de qualité, ses ressources ne lui permettent que d'assurer sa cyberprotection et sa cyberdéfense en situation normale et il n'est pas en mesure de gérer plusieurs cas simultanés, complexes ou de longue durée. En matière d'assistance, l'armée est ainsi en mesure de ne fournir que des prestations ponctuelles.

S'agissant du personnel de milice, le système actuel ne fait pas usage de son potentiel; un dispositif particulier – comme par exemple *SPHAIR* mis en place par les Forces aériennes afin de mieux identifier, tester, pré-instruire et recruter le personnel requis – est indispensable[4]. Des travaux allant dans ce sens sont en cours; ils montrent également qu'un système *classique* d'école de recrue / cours de répétition n'est pas adapté: on ne fabrique pas un informaticien en 4 mois. En l'état, les militaires sont recrutés et engagés isolément, sans possibilité de faire une carrière militaire dans le domaine cyber, comme cela se pratique par exemple pour le renseignement militaire. L'engagement de militaires en service long est profitable, mais ce sont de jeunes militaires avec peu de maturité, d'expérience et de formation devant être étroitement conduits. Des modèles d'engagement flexibles et différenciés, déjà pratiqués dans le passé comme par exemple dans l'ancien Service de Renseignement stratégique, seront à privilégier, avec l'encadrement professionnel nécessaire pour les gérer.

[3] https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173103

[4] L'avis de droit du Service juridique DDPS du 26.08.2014 montre que des citoyens avec un degré d'invalidité jusqu'à 40% pourraient faire service auprès de la cyberdéfense où ce sont avant tout les facultés intellectuelles qui sont requises.

1.6 Sensibilisation et instruction

La Sécurité des informations et des objets (SIO) est en charge de la sécurité intégrale pour le DDPS. Cette unité réalise entre autres diverses campagnes de sensibilisation, y.c. dans la sécurité informatique. Tout comme l'unité organisationnelle *Cyberdéfense armée*, la SIO est présente lors de séminaires dans les écoles de cadres et diffuses de nombreuses séquences d'instruction via le système LMS[5]. L'unité organisationnelle *Cyberdéfense armée* réalise quant à elle, sous l'appellation *ATTENZ!UN*, des campagnes de sensibilisation. Dans la mesure de ses moyens elle est également présente sur les lieux d'exposition de l'armée et instruit les unités militaires à l'engagement en fonction des besoins opérationnels. Les unités organisationnelles *cyber* du DDPS participent aux exercices *Cyber Coalition* (OTAN), *Locked Shield* (CCDCoE[6], Tallinn) et *Cyber Storm* et organisent également *Cyber Pakt*. Enfin, le réseau national de sécurité, rattaché au Secrétariat général du DDPS, a réalisé en 2016 l'exercice *Popula*.

L'unité d'action de tous ces efforts n'est cependant pas encore satisfaisante. Au sein de l'armée, l'instruction n'est pas à jour avec les cybermenaces et le sous-effectif des unités actives dans la cyberdéfense ne permet pas de fournir les produits dont la troupe a besoin dans la quantité et la qualité requises.

1.7 Gouvernance et conduite

Renforcement des mesures de protection

La SIO prépare les prescriptions de sécurité à l'attention de la / du Secrétaire général(e) du DDPS, mais il lui manque une image consolidée des cybermenaces. Il en résulte divers retards et décalages par rapport aux technologies et à la pratique courante des utilisateurs. On observe des inconsistances entre les directives et leur mise en œuvre laisse à désirer.

Pour répondre au problème général de la sécurité des systèmes et infrastructures TIC militaires et civils du DDPS, la SIO met en place avec les offices du DDPS un système de gestion de la sécurité de l'information (ISMS) selon la norme ISO 27000. Des efforts sont aussi en cours en matière d'architecture et de topologie des réseaux. Ces initiatives, ainsi que la mise en place d'un processus d'amélioration continue, contribueront à l'élévation du niveau de sécurité. Pour les piloter, la SIO dispose du *Fachorgan Informationssicherheit* (FINS) qui réunit les différents responsables de sécurité des offices. Une fois en vigueur d'ici environ 2019, la nouvelle Loi sur la sécurité de l'information (LSI) renforcera significativement l'effet de ces travaux. Le DDPS passera ainsi graduellement d'une logique de conformité (*compliance*) à une logique de vérification de l'efficacité des mesures de protection. La modernisation des systèmes et infrastructures TIC du DDPS[7] fait partie des améliorations générales en cours de réalisation.

L'Office fédéral de la protection de la population (OFPP) effectue de son côté, dans le cadre de la SNPC, des analyses de risques et de vulnérabilités des secteurs critiques. Il tient un inventaire des infrastructures critiques qui sert de base à leurs travaux de planification et de réalisation des mesures de protection nécessaires ainsi qu'à l'amélioration de leur degré de résilience. L'OFPP assure en outre la coordination de la mise en œuvre de la stratégie pour la protection des infrastructures critiques (PIC) qui comprend un secteur critique *Information et communication* traitant notamment des cyberrisques.

[5] Learning Management System (plateforme électronique d'instruction)

[6] Cooperative Cyber Defence Centre of Excellence; ce centre de recherche, qui n'effectue pas de tâches opérationnelles, est accrédité par l'OTAN. Il est localisé à Tallinn, en Estonie.

[7] http://www.vtg.admin.ch/fr/actualite/themes/programmes-projet/systemes-tic.html et https://www.efk.admin.ch/fr/publications/economie-administration/projets-informatiques/1481-pruefung-des-ikt-schluesselprojekts-fitania-eidgenoessisches-departement-fuer-verteidigung-bevoelkerungsschutz-und-sport-f.html

Conduite des projets

Tous les projets d'acquisition ne parviennent pas encore à considérer la protection contre les cyberrisques comme un impératif. Des faiblesses organisationnelles consécutives à la prise en compte insuffisante de cette dimension ont notamment été constatées lors des exercices *Conex* et *Stabante* en 2015. La pratique s'améliore toutefois, à l'image du projet d'acquisition du nouvel avion de combat[8]. La réalisation de projets dans le domaine de la cybersécurité est également encore trop lente en raison du manque de personnel qualifié et d'une compréhension générale insuffisante des cyberrisques. Les procédures en place ne permettent pas de réagir rapidement et une accélération de la réalisation des projets est nécessaire, notamment pour répondre à temps en cas d'incidents.

Coordination opérationnelle

MELANI OIC (Melde- und Analysestelle Informationssicherung, Operation Information Center) est une unité rattachée au Service de renseignement de la Confédération en coopération avec l'Unité de pilotage informatique de la Confédération (UPIC) dépendant du Département fédéral des finances. Cette unité assure la coordination opérationnelle des acteurs fédéraux de la cybersécurité et des infrastructures critiques. Sa tâche principale consiste à analyser la situation des cybermenaces. Elle assure la conduite de l'échange d'informations parmi environ 200 exploitants d'infrastructures critiques – y compris les fournisseurs de prestations de l'administration fédérale et l'armée – ainsi que l'appui opérationnel et analytique de la première heure au profit de ces entités en cas de cyberincident, pour autant qu'il s'agisse de situations ne pouvant pas être résolues dans le cadre courant ou qui menacent d'autres prestataires critiques.

Conduite de la cyberdéfense militaire

Les attaques subies en 2016 ont mis en évidence un niveau insuffisant des moyens de conduite, un manque de préparation pour répondre rapidement aux anomalies ainsi que des lacunes dans le monitoring de certains systèmes. L'état-major[9] militaire créé en 2013 renforce le noyau professionnel en termes de compétences et de capacité à durer; il permet l'intégration du domaine cyber dans les actions militaires à l'échelon opératif, mais ici également des progrès sont encore nécessaires. L'intégration du thème *cyber* dans les règlements militaires tel que la *Conduite tactique* et la *Conduite opérative* est réalisée et les procédures standards établies; toutefois la maturité de ces documents devra être améliorée au fur et à mesure des expériences pratiques.

1.8 Collaborations

Protection du Groupement Défense

La Stratégie nationale pour la protection de la Suisse contre les cyberrisques (SNPC) encourage les exploitants d'infrastructures critiques à travailler avec leurs partenaires et prestataires. Par rapport à ses propres missions, l'armée a identifié les prestataires critiques dont l'indisponibilité serait dommageable pour ses opérations. Elle a donc mis en place des collaborations avec eux pour la prévention[10] des cyberrisques. Pour être en mesure de gérer sur le long terme le sujet complexe de la cybersécurité, le DDPS doit par ailleurs s'appuyer sur des partenaires industriels et académiques. Une *cartographie* précise à ce sujet manque encore.

[8] Rapport du groupe d'experts - Prochain avion de combat, http://www.vbs.admin.ch/content/vbs-internet/fr/die-schweizer-armee/sicherheit-im-luftraum.download/vbs-internet/fr/documents/defense/sécuritéespaceaérien/Bericht-Luftverteidigung-der-Zukunft-f.pdf

[9] Le DDPS est le seul à disposer d'un tel état-major; ses membres apportent des compétences uniques.

[10] En cas de crise, ces collaborations sont remplacées par les processus opérationnels courants.

Partenaires étrangers civils

Dans le domaine du contre-renseignement cyber, le besoin de coopérer est fort. En effet, les cyberincidents ont toujours une composante internationale et aucun pays ne peut avoir du succès en restant isolé. Le Service de renseignement de la Confédération (y.c. MELANI OIC) maintient une longue tradition de coopération internationale en matière de renseignement, y.c. en matière de cybermenaces. Il participe depuis des années, en plus des échanges réguliers avec les services partenaires, aux travaux de diverses instances spécialisées et maintien également ses contacts en participant aux exercices tels que *Cyber Storm* (USA) et *Cyber Europe* (ENISA).

Partenaires étrangers militaires

L'armée entretient des relations avec plusieurs forces armées étrangères. Ces échanges sont essentiels pour élargir le champ des connaissances et procéder à des comparaisons. Les contacts restent toutefois limités par les ressources disponibles, mais la volonté de les développer est affichée. Un renforcement est d'ailleurs en cours avec le CCDCoE. La Suisse, déjà présente avec des stagiaires, est candidate pour devenir *Contributing Nation* à ce centre de recherche.

Institutions de recherche et universitaires

Les institutions académiques suisses (formation, recherche et innovation) sont nombreuses et leurs compétences sont élevées. A quelques exceptions près, elles restent cependant largement sous-utilisées dans le développement de la cyberdéfense. Le DDPS a réalisé en 2015 un premier inventaire au profit de la SNPC et il confiera prochainement sa mise à jour à l'Académie suisse des sciences techniques (SATW). Le DDPS attribue aussi divers mandats de recherche et d'appui dans des domaines techniques[11] et non techniques aux hautes écoles. C'est par exemple le cas avec le *Center for Security Studies* (CSS) de l'EPFZ. Les experts du DDPS soutiennent également les travaux de recherche d'étudiants (bachelor, master, doctorat) et s'engagent aussi en tant que coachs ou juges lors de concours comme le *Cyber Student Challenge* organisé par le *Geneva Center for Security Policy* (GCSP). Enfin, l'armée apporte depuis peu son soutien à *Swiss Cyber Storm*[12], une manifestation pour détecter et encourager des jeunes talents.

2 CADRE DE PLANIFICATION DU PLAN D'ACTION CYBERDEFENSE

Les éléments suivants ont encadré l'élaboration du plan d'action.

Objectif opérationnel

Le DDPS est un pôle reconnu en matière de cyberdéfense. En étroite collaboration avec ses partenaires, l'économie et les hautes écoles, il dispose des moyens suffisants en quantité et qualité, afin de:

- protéger, défendre et assurer la résilience en tout temps et toute circonstance de ses systèmes et infrastructures TIC contre les cybermenaces et cyberattaques;
- conduire les opérations militaires et de renseignement dans le cyberespace;
- prêter assistance aux autorités civiles en cas de cyberattaques contre les infrastructures critiques.

Objectif temporel

Trois étapes clés ont été fixées:

[11] A l'exemple d'une nouvelle approche de détection de cyberattaques développée en commun https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-67019.html

[12] https://www.swisscyberstorm.com/

- d’ici fin 2018, optimiser les moyens existants pour assurer une protection renforcée des infrastructures TIC du DDPS et soutenir la révision de la SNPC;
- d’ici fin 2018, faire du DDPS un acteur capable de se défendre efficacement et un prestataire crédible, capable de prêter assistance aux autorités demanderesses (subsidiarité).
- d’ici à fin 2020, doter le DDPS de la capacité à agir dans le cyberespace en cas de crise majeure.

Lignes directrices

Les éléments de détail suivants ont encadré le développement:

- se limiter aux missions, compétences et moyens du DDPS (selon les bases légales et l'analyse des tâches sous chi. 1.4);
- s'inscrire dans l'esprit de la SNPC pilotée par le DFF;
- développer des solutions flexibles et endurantes capables d'évoluer continûment et sur le long terme;
- formuler les missions des unités du DDPS afin d'assurer la protection, la défense et la résilience en tout temps et toute circonstance de ses propres systèmes et infrastructures TIC;
- formuler les missions de l'armée pour assurer ses tâches d'assistance (subsidiaire) au profit d'infrastructures critiques subissant des cyberattaques ainsi que ses tâches en cas de conflit / guerre;
- pour autant qu'il y ait un gain démontré, concentrer les moyens, structurellement / organiquement ou dans le cadre des processus;
- établir une coopération solide avec l'industrie et les institutions de formation, recherche et innovation;
- régler en particulier la gouvernance, les processus, la formation, l'emploi de la milice, et formuler les besoins en ressources en fonction du niveau d'ambition retenu et contribuer au rétablissement d'une culture de la sécurité.

3 ARCHITECTURE DU PLAN D'ACTION CYBERDEFENSE

3.1 Capacités

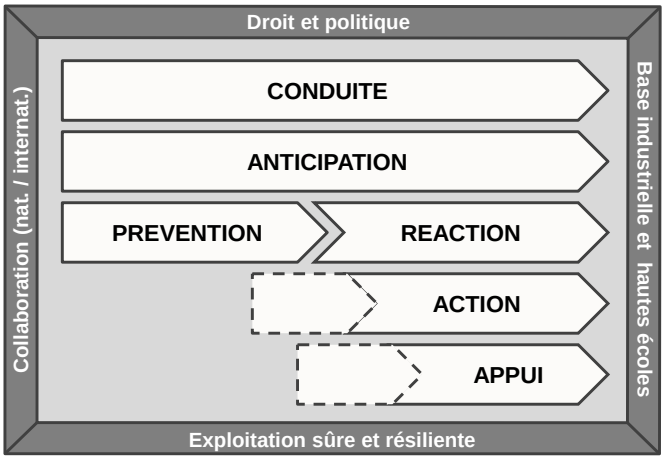
Le Plan d'action cyberdéfense est à considérer dans un ensemble comprenant:

- le **cadre légal** (lois, ordonnances) et les décisions politiques (décisions du Conseil fédéral, ordres, directives, interventions parlementaires, recommandations des organes de contrôle, stratégies telles que Rapport de politique de sécurité, Stratégie nationale pour la protection de la Suisse contre les cyberrisques et Stratégie nationale pour la protection des infrastructures critiques);
- un **réseau de collaborations** en Suisse et à l'étranger afin d'échanger des informations sur les menaces, les bonnes pratiques, etc.;
- un **réseau des compétences** disponibles en Suisse (en priorité) dans la base industrielle technologique et les hautes écoles;
- un **socle** de systèmes et d'infrastructures TIC (prestations propres et celles externes dont le DDPS est dépendant) sûrs et résilients afin que les moyens de défense puissent concentrer leurs efforts sur les prestations vitales.

Afin de réaliser son objectif stratégique dans le contexte décrit ci-dessus, le DDPS doit disposer / perfectionner les capacités suivantes:

- **conduite** des mesures et actions à tous les échelons concernés, en permanence et en toute circonstance, ainsi que la coordination avec les instances et partenaires extérieurs, pour les tâches concernant directement le DDPS;

- **anticipation** du développement et de l'occurrence des menaces liées au cyberespace afin de disposer à temps des éléments décisionnels requis;
- **prévention** afin de réduire l'exposition du DDPS aux cyberrisques;
- **réaction** afin de limiter les conséquences éventuelles d'incidents, au besoin par des contre-mesures offensives;
- **action** dans le cyberespace au profit des propres opérations de défense et de renseignement;
- **appui** aux autorités civiles compétentes, en priorité dans le cadre de la défense des infrastructures critiques.



3.2 Principes de compétences au sein du DDPS

Les principes suivants régissent les activités au sein du DDPS:

Gouvernance

- En raison de l'interaction de nombreux intervenants dans et hors du DDPS, le pilotage de la cybersécurité du DDPS est assuré à son niveau politique.

Protection dans le cyberespace

- Le principe de propre responsabilité de chaque entité est cardinal; le DDPS n'est ainsi responsable que de la protection de ses systèmes, infrastructures et processus propres.
- Le DDPS définit les spécifications et procède à l'homologation des composantes sensibles nécessaires à l'implémentation des solutions de haute sécurité dont il dépend.
- Conformément à la SNPC, les offices du DDPS, notamment le Service de renseignement de la Confédération[13] et l'armée, collaborent avec les opérateurs d'infrastructures critiques dont ils sont dépendants pour renforcer leurs mesures d'anticipation et de prévention.

Défense dans le cyberespace

- Les cyberattaques dirigées contre la population et l'économie sont du ressort des autorités fédérales et cantonales compétentes. Le Service de renseignement de la Confédération accomplit ses tâches originaires de prévention et de détection. En cas de cyberattaques d'un Etat contre notre population ou notre économie dans les domaines définis par la LRens (par exemple espionnage ou terrorisme), le Service de renseignement de la Confédération assure l'identification de ces attaques et de leurs auteurs ainsi que la défense des cibles potentielles.
- L'armée assure la défense de ses propres systèmes et infrastructures TIC. En temps de paix, les contre-mesures actives (*Abwehr*) de l'armée au profit de ses propres systèmes et infrastructures TIC sont soumises à autorisation[14].

[13] Basé sur les décisions du Conseil fédéral de 2004 et 2007 et la mission spécifique de réaliser cet effort en coopération avec le DFF.

[14] Art. 100 al. 1 lit. c LAAM; l'ordonnance y relative devrait entrer en vigueur à mi-2018.

- Lorsque des infrastructures critiques civiles subissent des cyberattaques les contre-mesures actives éventuelles pour les faire cesser sont du ressort du Service de renseignement de la Confédération et soumises à autorisation[15].
- L'armée peut apporter son aide au Service de renseignement de la Confédération ou à d'autres autorités civiles sur instruction des autorités politiques. Cette aide peut être organisée au moyen d'accords de prestations (en particulier avec le Service de renseignement de la Confédération) ou être de nature subsidiaire.

Actions dans le cyberespace

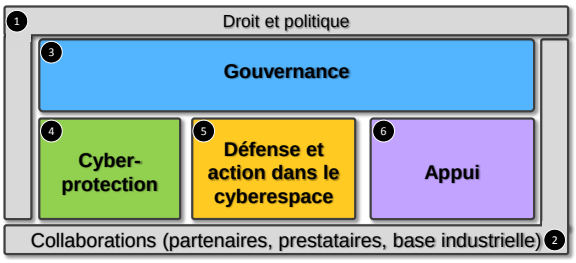
- Le Service de renseignement de la Confédération accomplit ses tâches originaires de renseignement dans et sur le cyberespace sur la base de la Loi sur le renseignement.
- L'armée est capable – comme elle le fait dans les autres sphères d'opération (air, terre, électromagnétique) – de mener des actions dans le cyberespace contre des systèmes et infrastructures TIC ennemis en cas de conflit (conformément au Droit international humanitaire).

3.3 Prestations d'appui de l'armée (aide subsidiaire)

Lorsque l'armée se voit confier des tâches hors de son champ d'action originaire, les critères suivants doivent être remplis avant de les accomplir:

1. L'engagement de moyens de l'armée ne doit pas compromettre la protection et la défense de ses propres systèmes et infrastructures TIC.
2. L'engagement de moyens de l'armée au profit de tiers n'est envisageable que pour des tâches réclamant des compétences dont elle a elle-même l'usage pour accomplir ses missions originaires.
3. L'armée ne prête son assistance technique aux autorités civiles que si celles-ci ont épuisé les possibilités à leur disposition.
4. Toute tâche de l'armée qui dépasse les critères 1 à 3 n'est possible qu'en attribuant à cette dernière les ressources dédiées nécessaires.

3.4 Architecture fonctionnelle



L'analyse de détail et la somme des expériences du DDPS depuis 2002 dans la sphère opérationnelle cyber ainsi que la structuration des capacités et compétences énumérées aux chap. 3.1 et 3.2 ont conduit à l'architecture fonctionnelle. Celle-ci est subordonnée au cadre normatif supérieur ❶ et appuyée par l'ensemble des collaborations ❷ du domaine cyber, réseau par excellence.

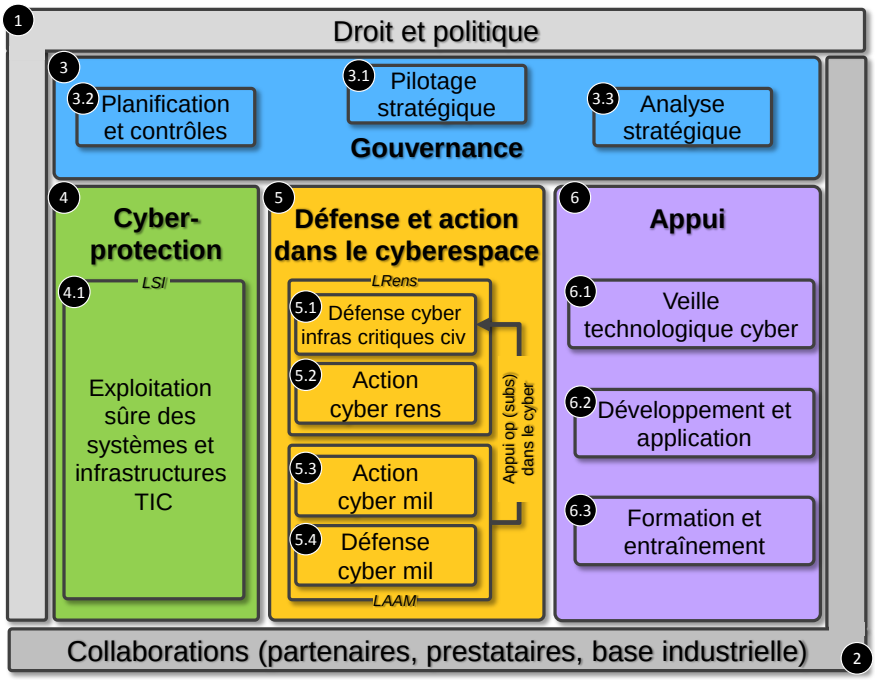
Elle se compose de quatre domaines:

- La **gouvernance** ❸ qui, à l'échelon stratégique du DDPS, crée les conditions favorables au développement et à l'engagement des moyens opérationnels et assure par ses activités de planification et de contrôle (y.c. selon la future LSI) que le niveau de sécurité requis est atteint.
- La **cyberprotection** ❹ où sont produites les prestations originaires des offices du DDPS et où se trouvent les exploitants de systèmes et infrastructures TIC du DDPS qui mettent en œuvre les directives de sécurité précitées sous ❸.

[15] Art. 26 al. 1 lit. d chiffre 2 LRens; Art. 37 al. 1 LRens

- La **défense et action dans le cyberespace** ❺ où le SRC et l'armée délivrent leurs effets respectifs dans le cyberespace au profit de leur défense propre et de leurs tâches originaires (renseignement et actions militaires).
- L'**appui** ❻ où sont produits de manière flexible le savoir, le personnel, les compétences et capacités techniques au profit des autres domaines (❸,❹,❺).

Ces domaines se subdivisent en **fonctions** selon la figure et le tableau suivants.



	Fonctions	Description des tâches / responsabilités
Gouvernance	3.1 Pilotage stratégique	Etablissement de la stratégie en matière de cybersécurité. Création des conditions cadre de prévention des crises de nature cyber et gestion de celles-ci ainsi que de leurs conséquences (mesures) au niveau DDPS.
	3.2 Planification et contrôles	Définition, sur la base d'une image claire des défis cyber, des mesures de sécurité et contrôle de leur application (via p.ex. des inspections et audits).
	3.3 Analyse stratégique	Suivi analytique continue des défis du cyber; établissement de l'image intégrale pour le DDPS sous l'angle des politiques, stratégies, technologies, recherches, doctrines, événements, etc, notamment par agrégation des produits issus des domaines 4, 5 et 6 pour disposer à temps des bases pour la prise de décision stratégique.
Protection (cadre *in prep*: Loi sur la sécurité de l'information)	4.1 Exploitation sûre[16] des syst. et infrastructures TIC du DDPS	Mise en œuvre des directives de sécurité selon fonction 3.2 afin d'assurer le niveau de sécurité et la résilience des offices du DDPS (en priorité SRC et armée) leur permettant de garantir en tout temps et toute circonstance l'accomplissement de leurs missions. Comprend la surveillance des propres infrastructures et systèmes TIC, l'intervention de premier niveau en cas d'incident et la gestion des vulnérabilités.
Défense et action dans le cyberespace (cadre: Loi sur le renseignement pour 5.1 et 5.2, Loi militaire pour 5.3 et 5.4)	5.1 Défense cyber des infra critiques civiles	Ensemble des interventions (selon LRens) au profit d'opérateurs d'infrastructures critiques subissant des cyberattaques; sur le plan capacitaire, le SRC peut s'appuyer sur la fonction 5.2 et les fonctions 5.3 et 5.4 (selon accord préalable de prestation ou subsidiairement).
	5.2 Actions cyber rens	Ensemble des actions (selon LRens) pour découvrir, qualifier ou attribuer des cyberattaques ainsi que pour appuyer les tâches courantes de renseignement.
	5.3 Actions cyber militaires	Ensemble des actions défensives et offensives (selon LAAM) produites par le domaine Défense au profit d'une opération militaire et/ou du renseignement militaire. En temps de paix, cette fonction soutient prioritairement la défense cyber militaire (fonction 5.4) et le SRC (fonctions 5.1

[16] Protection de la confidentialité, de l'intégrité et de la disponibilité des systèmes et services.

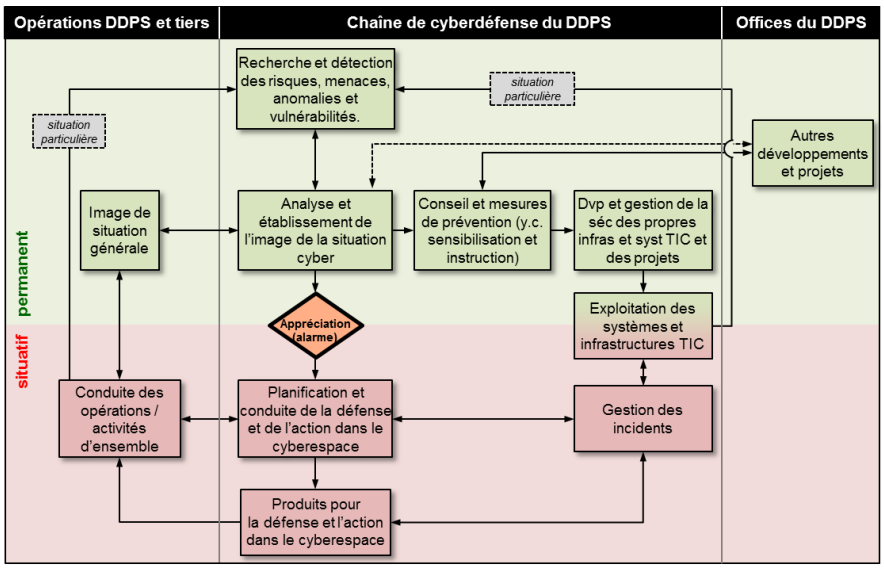
	Fonctions	Description des tâches / responsabilités
		et 5.2).
	5.4 Défense cyber militaire	Ensemble des actions techniques et non-techniques (selon LAAM) pour prévenir, réduire et faire cesser les actions hostiles contre les systèmes et infrastructures TIC de l'armée et assurer sa capacité à remplir ses missions originaires. Cette fonction peut soutenir les fonctions 5.1 à 5.3.
Appui	6.1 Veille technologique cyber	Suivi des développements technologiques relatifs au cyber afin d'établir une image globale et en déduire des conséquences pour soutenir les développements du DDPS.
	6.2 Développement et application	Plateforme commune au DDPS, à l'industrie, aux opérateurs d'infrastructures critiques et hautes écoles pour développer des cyberoutils de sécurité engageables dans les domaines 4 et 5 et disposer d'une réserve en personnel et de compétences engageables de manière agile.
	6.3 Formation - entraînement	Recrutement et préparation des métiers du cyber des domaines 3, 4 et 5, en étroite coopération avec les hautes écoles; comprend l'établissement d'une réserve de personnel technique (6.2) et non technique.

4 RÉALISATION DU PLAN D'ACTION CYBERDEFENSE

4.1 Processus

L'expérience, notamment celle gagnée lors de l'exercice *Cyber Pakt* 2016, a permis d'uniformiser les pratiques et de structurer les processus opérationnels clés (le ***comment ça marche***) à l'échelle du DDPS. Il a été ainsi possible de définir l'intégration des prestations de l'armée, notamment pour répondre à la SNPC en matière d'aide subsidiaire. Un de ces processus est spécifiquement dédié à la défense des infrastructures critiques en cas de cyberattaque. L'opérateur agressé adresse alors sa demande à l'autorité civile responsable puis MELANI OIC la traite, réalise l'analyse de base et transmet le cas aux acteurs chargés de délivrer les produits de défense, tel que l'armée si les critères sont remplis (voir chi. 3.3).

Ces processus (voir figure ci-dessous), sont articulés <u>verticalement</u> (le "*qui*") et <u>horizontalement</u> (le "*quand*") et peuvent se lire comme suit:



<u>En permanence:</u> la *chaîne de cyberdéfense* du DDPS recherche avec son réseau de partenaires et ses senseurs toute forme de menace et d'agression contre ses systèmes et infrastructures TIC dans le cyberespace. Sur cette base est établie l'image de la situation cyber lui permettant de:

- alarmer et/ou conseiller les services en charge de l'exploitation des propres infrastructures TIC et des projets (y.c. chez les tiers et partenaires au besoin) afin que ceux-ci prennent les mesures nécessaires pour leur protection;

- alarmer les opérations quant à des cyberévénements pouvant affecter leurs activités et, si cela est pertinent, informer d'autres autorités compétentes;
- contribuer à l'image de la situation cyber des voisins;
- assurer (à temps) le développement continu des propres capacités cyber et la formation du personnel;

En cas de besoin, lors d'événements ou commandé par un échelon supérieur:

- soutenir les activités de planification et de conduite et synchroniser la sphère d'opération cyber avec les autres domaines;
- fournir aux destinataires les produits de cyberdéfense autorisés.

4.2 Ressources requises

Personnel professionnel

Au total 166 postes sont prévus, dont 21 pour la partie *appui*. A l'exception des fonctions 6.1 à 6.3, toutes les fonctions de l'architecture sont déjà dotées de moyens de base fonctionnels – environ 65 postes d'ici à fin 2017 – que les quelques 100 nouvellement réalloués viendront renforcer, sans modification des structures du DDPS.

La détermination d'un effectif cible précis n'est pas possible, la nature même des cybermenaces et des incidents ne le permettant pas. Ce chiffre a donc été élaboré sur la base des critères suivants:

- atteindre une structure stable disposant de toutes les composantes *métier* requises; tout renoncement entraînant alors des lacunes capacitaires et donc des risques longs et délicats à gérer;
- répondre à plusieurs événements simultanés, d'envergure et/ou complexes;
- disposer de moyens en suffisance pour éliminer rapidement les vulnérabilités existantes et en éviter de nouvelles découlant de la digitalisation omniprésente;
- disposer de la capacité à accompagner les prochaines grandes acquisitions et ainsi éviter que se créent des *vides cyber*;
- anticiper et non plus subir le développement rapide des défis du cyberespace,
- disposer d'une taille critique permettant d'offrir des perspectives de développement de carrière au personnel engagé dans la branche.

Ces effectifs serviront intégralement à la production quotidienne de sécurité pour le compte du DDPS et des opérateurs d'infrastructures critiques. Ils ne comprennent pas de fonction de soutien (p.ex. personnel, finances, sécurité, logistique), ces tâches étant assurées par les unités organisationnelles existantes.

Personnel de milice

Les effectifs professionnels, à l'exception de ceux du Service de renseignement de la Confédération, seront renforcés par des militaires de milice. La planification de détail sera établie dans le cadre du concept du *CYD-Campus*. Comme évoqué au chi. 1.5, des modèles d'engagement différenciés seront privilégiés et ces militaires deviendront des spécialistes intéressants aussi pour le secteur privé.

Finances

En l'état des travaux, une planification détaillée ne peut pas être établie. Il incombe à chaque unité organisationnelle de déterminer ses besoins et de les intégrer aux processus ordinaires. Il ne sera donc pas mis en place de processus spécifique *cyber*. En termes d'ordre de grandeur et sur la base de ce que pratiquent les nations considérées, on peut estimer le coût de l'instrument de cyberdéfense, personnel compris et une fois atteinte sa capacité opérationnelle, à environ 2% du budget annuel du DDPS.

4.3 Mesures pour la réalisation du PACD

Le PACD comprend 11 projets partiels et sa réalisation durera jusqu'en 2020. La vitesse de sa réalisation dépendra essentiellement de la capacité du DDPS à réallouer au projet les postes[17] nécessaires.

Projets partiels	Objectifs	Resp.	Délai (état)[18]
1) Sécurité de l'information	Concrétiser la fonction *planification et contrôles* (3.2) de l'architecture. Tenir compte du développement de la Loi sur la sécurité de l'information (LSI) et de la réalisation de l'ISMS.DDPS.	SG DDPS SIO	Fin 2017 (optimisation en cours)
2) Cellule cyberdéfense DDPS (CYD DDPS)	Concrétiser les fonctions *pilotage stratégique* (3.1) et *analyse stratégique* (3.3) de l'architecture. Intégrer les recommandations de la Révision interne DDPS. Assurer la continuité entre cyberprotection et cyberdéfense par une étroite collaboration avec SIO. Assurer la cohérence entre CYD DDPS, le Beirat CYD VBS et CYD-Campus.	SG DDPS Dél CYD	Mi-2017 (opérationnel, délégué désigné, premiers collaborateurs engagés)
3) Moyens cyber du SRC	Concrétiser les fonctions *cyberdéfense des infra critiques civiles* (5.1) et *opérations cyber rens* (5.2) de l'architecture.	SRC	Fin 2017 (opérationnel selon niveau actuel)
4) Moyens cyber de l'armée	Concrétiser les fonctions *actions cyber militaires* (5.3) et *défense cyber militaire* (5.4) de l'architecture.	Armée BAC	Fin 2017 (selon niveau op actuel)
5) CYD-CAMPUS	Concrétiser les fonctions *veille technologique cyber* (6.1), *développement et application* (6.2) et *formation – entraînement* (6.3) de l'architecture; intégrer armasuisse S+T; couvrir en priorité la période 2018-2019 et devenir le plus rapidement possible fonctionnel.	SG DDPS Dél CYD	Fin 11.2017 (concept de base)
6) Développement et gestion du personnel professionnel	Assurer le renforcement quantitatif / qualitatif des effectifs; les effectifs seront générés par réallocations internes; à cet effet il faudra: - envisager de possibles reports ou abandons de tâches sans mettre en danger la réforme de l'armée ou les acquisitions en cours; - absorber simultanément la réduction d'effectifs voulue par le Parlement; - privilégier une élévation régulière et ordonnée des effectifs afin d'amortir l'effort et de faciliter les tâches de recrutement, d'intégration, d'instruction et d'organisation.	SG DDPS Ressources	Fin 2017 (planification en cours; montée en puissance jusqu'en 2020; les projets partiels adaptent leur évolution en fonction du rythme d'acquisition des postes)
7) Développement et gestion du personnel de milice	Assurer le recrutement, la gestion et le développement du personnel de milice, considérer notamment les expériences du programme SPHAIR et les concours tels que Swiss Cyber Storm, synchroniser avec le projet 5, intégrer les besoins à la révision OA 2019.	Armée BAC	Fin 2017 (opérationnel selon niveau actuel)
8) Instruction et sensibilisation du personnel	Assurer la formation de base et continue des différentes catégories de personnels du DDPS (à l'exception du SRC qui forme son personnel lui-même); synchroniser avec les projets 5, 6, 7.	armée BAC	Fin 2017 (partiellement opérationnel)
9) Infrastructures	Co-localiser les moyens CYD du DDPS (sauf	armée	Fin 2017

[17] Le plafonnement décidé par le Parlement en décembre 2016 implique une réduction de quelques 300 postes pour le DDPS. Avec la cyberdéfense, l'effort global est donc de l'ordre de 400.

[18] Il s'agit du délai de la planification de détail, non de l'achèvement des travaux, celle-ci étant prévue jusqu'en 2020. La difficulté à générer les postes nécessaires par transferts internes, ainsi que la cyberattaque subie durant l'été 2016 (http://www.vbs.admin.ch/content/vbs-internet/fr/die-schweizer-armee/schutz-vor-cyber-angriffen.detail.nsb.html/68135.html) ont provoqué un retard de 4-5 mois sur le plan horaire initial.

Projets partiels	Objectifs	Resp.	Délai (état)[18]
CYD	SRC); synchroniser avec le projet 5.	BAC	
10) Cadre réglementaire militaire	Il s'agit de - régler les interfaces entre l'armée et le SRC; - transposer l'article 100, et notamment l'al. 1, let. c LAAM dans une ordonnance; - finaliser la base doctrinale et sa transposition dans un règlement cyber de l'armée; - transposer la nouvelle organisation dans le règlement administratif de la BAC; - élaborer une directive cyber du CdA réglant le fonctionnement de la sphère cyber au sein de l'armée.	armée BAC	Fin 2017
11) Amélioration continue	Il s'agit de garantir l'amélioration continue du dispositif cyberdéfense du DDPS avec un processus adapté de mesure de la maturité.	SG DDPS Dél CYD	Fin 2017

4.4 CYD-Campus

Les compétences et l'échange d'informations constituent un pivot du PACD avec a) les partenaires opérationnels nationaux et internationaux, b) la base industrielle technologique et c) les hautes écoles. Un tel échange a toutefois besoin de plus qu'une déclaration d'intention. Il faut en effet que les différents acteurs se connaissent et agissent de concert au quotidien. Il faut pour cela raccourcir les distances et établir un *pôle de ralliement* pour la cyberdéfense baptisé *CYD-Campus* qui:

- établisse une **plateforme d'anticipation** qui profite à l'ensemble des acteurs de la cyberdéfense en Suisse;
- renforce, dans une approche de partenariat public-privé, les **compétences et capacités technico-opératives** du DDPS afin de lui permettre de prêter assistance aux opérateurs d'infrastructures critiques durablement, agilement, avec les compétences requises;
- renforce la capacité des acteurs suisses de la cyberdéfense à agir de concert en assurant leur **interopérabilité**;
- attire et gère les **talents** dans le domaine de la cyberdéfense et crée une communauté dynamique.

Différents conflits d'intérêts compliqueront la création du *CYD-Campus*. Il faudra faire coexister plusieurs degrés de confidentialité et des matières opérationnelles ou académiques n'ayant pas les mêmes besoins et buts. Il s'agira aussi de veiller à ne pas créer de doublons. Le projet devra délivrer ses premiers effets dès 2018, atteindre une capacité opérationnelle de base dès mi-2019 et sa pleine capacité à fin 2020. Il devra permettre en tout temps au DDPS d'utiliser ses compétences et capacités pour assister les opérateurs d'infrastructures critiques.

L'instruction du personnel sera un élément particulièrement important pour diminuer l'exposition du DDPS et de l'armée aux cyberrisques. Il s'agit donc de former continuellement le personnel professionnel et de milice aux défis et menaces du cyberespace dès leur engagement et tout au long de leur carrière.

4.5 Conduite de la réalisation

La réalisation du PACD comprend 3 domaines d'action:

- les **moyens** pour doter les unités concernées de la capacité à remplir leurs missions;
- les **processus** pour obtenir à tout moment de la part des moyens disponibles la plus grande efficacité possible;

- les **compétences** en complétant le dispositif avec les parties *gouvernance* et *appui* afin de renforcer les moyens et d'assurer une conduite homogène des processus.

La réalisation du PACD durera jusqu'à fin 2020, ce qui nécessitera – en raison de la rapide évolution du cyberespace – sa vérification et son adaptation continue. La direction générale du projet sera assurée par le Délégué cyberdéfense DDPS et la surveillance confiée au Conseil de l'informatique DDPS (IR VBS). Enfin les éléments du PACD concernant le domaine Défense seront intégrés au Masterplan géré par l'Etat-major de l'armée.

5 CONCLUSION

Le DDPS, comme acteur majeur de la politique de sécurité, doit relever, avec ses partenaires, les défis complexes et innombrables de la transformation numérique de la société et les intégrer dans le cadre de ses missions. En raison de la rapidité de l'évolution de ce domaine, le développement des capacités de cyberdéfense ne peut pas attendre. De bonnes bases ont été établies, mais malgré les récents progrès il reste beaucoup à faire.

Le Plan d'action cyberdéfense est la feuille de route initiale du DDPS pour répondre concrètement et pragmatiquement aux défis multiples que le cyberespace pose à notre politique de sécurité.