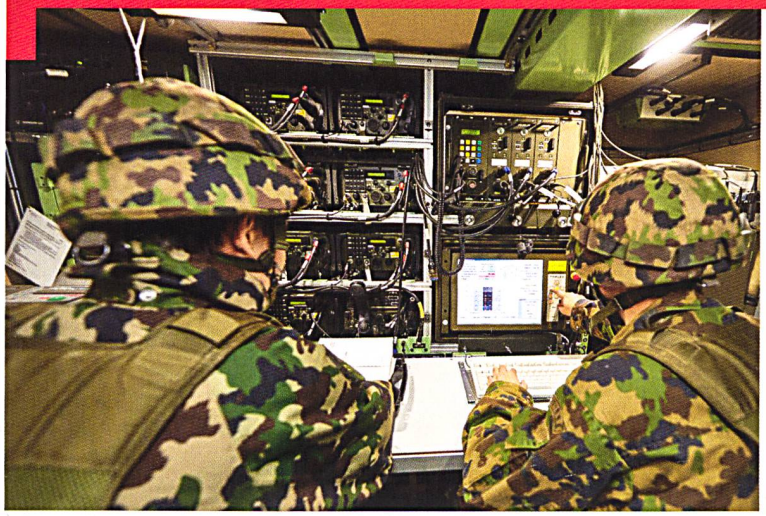
Zeitschrift: Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: Le plan d'action cyberdéfense du DDPS (PACD)
Autor: Vernez, Gérald
DOI: https://doi.org/10.5169/seals-823446



Les communications et les systèmes d'information de l'armée sont bien protégés. Mais qui est responsable de la protection des réseaux de l'administration fédérale ?

Cyber

Le plan d'action cyberdéfense du DDPS (PACD)

Gérald Vernez
Délégué du DDPS pour la cyberdéfense

En juillet 2016, motivé par la cyberattaque subie par RUAG et découverte en janvier, une révision du dispositif cyber du DDPS a été ordonnée. L'état des lieux et la stratégie ont été approuvés fin octobre 2016 et le plan de réalisation en juin 2017. Le PACD était né. Que règle-t-il, quel est sa place dans le dispositif national, qu'entend-t-on par subsidiarité, quels sont les moyens consacrés ? Le présent article met l'accent sur les éléments clés de ce plan interne au DDPS,[1] fondé sur ses propres bases légales et moyens.

Tâches et position de la cyberdéfense

Les prestations dont le DDPS a la charge en matière de cybersécurité[2] sont résumées ci-contre. Elles résultent de la Stratégie nationale pour la protection de la Suisse contre les cyberrisques (SNPC; que le PACD complète)[3] ainsi que de la mise en œuvre de la Loi sur le renseignement[4] et de la Loi sur l'armée et l'administration militaire.[5] La motion 17.3507,[6] approuvée en mars par le Parlement, confère par ailleurs aux éléments du PACD concernant l'armée une solide légitimité politique.

Sur la base de ces tâches et d'un état des lieux exhaustif a été formulé l'objectif opérationnel suivant :
«*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.

Pour la SNPC, le principe de la responsabilité individuelle est un élément cardinal ; la cybersécurité est ainsi décentralisée, à la charge de chaque individu, entreprise ou institution. L'Etat n'intervient alors que subsidiairement et, dans le cas de l'armée, uniquement si les critères suivants sont remplis :
- l'engagement de moyens de l'armée ne doit pas compromettre la protection et la défense de ses propres systèmes et infrastructures TIC ;
- 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 ;
- l'armée ne prête son assistance technique aux autorités civiles que si celles-ci ont épuisé les possibilités à leur disposition.

Le DDPS : Un système

Le dispositif de cyberdéfense du DDPS est constitué de fonctions articulées dans une architecture résumée ci-contre. Encadré par les règles qui guident son action et les collaborations qui le soutiennent, le dispositif du DDPS comporte quatre éléments clés : le pilotage qui assure la cohérence de l'ensemble, la protection qui comprend l'exploitation sûre des systèmes et infrastructures TIC

1 https://www.vbs.admin.ch/content/vbs-internet/fr/die-schweizer-armee/schutz-vor-cyber-angriffen.download/vbs-internet/fr/documents/defense/cyberattaques/Aktionsplan-Cyberdefense-f.pdf

2 Ce terme décrit l'état recherché en matière de situation IT où les risques sont réduits à un niveau supportable par un ensemble de mesures passives et actives.

3 Le Conseil fédéral a confié au Département fédéral des finances son élaboration et le pilotage de sa réalisation www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/ncs_strategie.html.

4 Loi sur le renseignement (LRens, art. 26 al 1 lit. d chiffre 2 et art. 37 al. 1).

5 Loi sur l'armée et l'administration militaire (LAAM, art. 100 al. 1 lit. c)

6 17.3507 Motion Dittli - Création d'un commandement de cyberdéfense dans l'armée suisse: https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507 ; le texte original basé sur les ammendements proposés par la Commission de politique de sécurité du Conseil national se trouve sous https://www.parlament.ch/centers/kb/Documents/2017/Rapport_de_la_commission_CPS-N_17.3507_2017-10-30.pdf

En matière de ...

Prestations du DDPS au profit ...	cyberprotection	cyberdéfense (Abwehr)	actions dans le cyberespace
des individus	Responsabilité individuelle	En cas d'incident intervention de la chaine de poursuite pénale	
de l'économie	Responsabilité des entreprises, selon les standards des régulateurs et des branches	En cas d'incident intervention de la chaine de poursuite pénale; soutien évtl. du DDPS pour les incidents de haute criticité	
des opérateurs d'infrastructures critiques	Responsabilité des opérateurs, selon les standards des régulateurs et des branches; appui du DDPS à titre préventif	Responsabilité des opérateurs ; le Service rens **peut** aider en cas de cyberattaque; si les conditions sont remplies l'armée **peut** appuyer	
du DDPS lui-même	Responsabilité du DDPS selon les standards de la Confédération et les besoins accrus du DDPS	Défense des propres systèmes et infrastructures TIC	Acquisition d'information et effets opérationnels dans le cyberespace

du DDPS, la défense qui englobe les actions dans le cyberespace et l'appui chargé de créer les conditions favorables en matière d'anticipation, de compétences et de capacités ainsi que de formation et d'entraînement.

Cinq des sept unités administratives du DDPS contribuent directement au PACD :

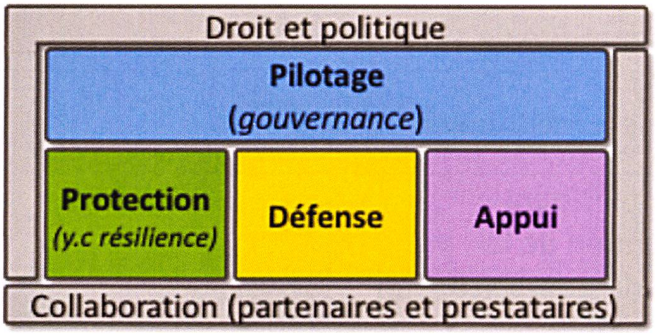
- le Secrétariat général du DDPS (SG DDPS) avec notamment le Délégué DDPS à la cyberdéfense et la sécurité des informations et des objets ;
- le Service de renseignement de la Confédération (SRC) avec différents services dont la partie de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) qu'il héberge ;
- l'Armée avec en particulier la Base d'aide au commandement qui exploite les systèmes et infrastructures du DDPS et dispose des compétences et capacités opérationnelles et techniques ;
- l'Office fédéral de la protection de la population responsable de la stratégie pour la protection des infrastructures critiques et chargé par la SNPC des études de risque ;
- armasuisse responsable des acquisitions et dont la division Sciences et Technologies joue un rôle central pour le développement et l'anticipation.

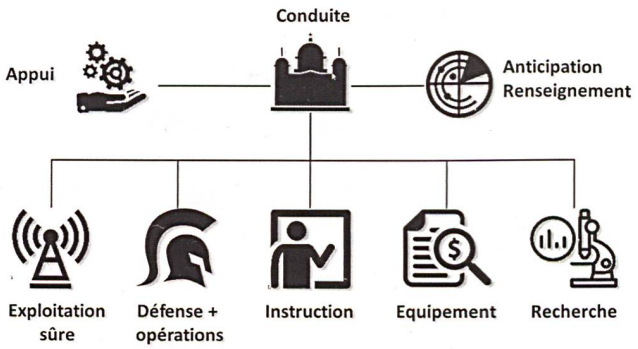
L'observateur non avisé pourrait y voir une fragmentation. Dans les faits, le DDPS dispose ainsi d'une boîte à outils complète (voir la figure ci-contre) qu'il peut, grâce au pilotage, mettre en œuvre de manière situative en concentrant les effets.

Réalisation du PACD

Le DDPS produit déjà au quotidien de la sécurité dans le domaine cyber et le PACD a pour but d'optimiser et de renforcer l'existant en termes de moyens, de processus et de compétences / capacités. L'état final recherché doit être atteint fin 2020 et devrait, en l'état, coûter annuellement environ 2% des ressources du DDPS. Le travail pour y parvenir est colossal, mais quelques exemples autorisent toutefois déjà un certain optimisme.

Gestion de crise : le DDPS est fort de son savoir-faire d'état-major et dispose avec ses cadres de milice de renforts considérables. L'expérience engrangée ces dernières années, en particulier avec les attaques contre RUAG en 2016 et l'armée durant l'été 2017, a permis d'établir des processus qui articulent les moyens et les actions du niveau technique à celui politique; fort de ce savoir, les experts du DFAE et du DDPS ont ainsi remporté





le premier rang du volet stratégique de l'exercice *Locked Shield 2018*.[7]

Instruction: le DDPS, grâce à l'armée, réalise de nombreuses activités de sensibilisation et forme déjà son personnel et de nombreux militaires aux rudiments de la cyberhygiène. La Base d'aide au commandement vient de lancer le cours « experts en cybersécurité » qui pourra déboucher pour les militaires sur une certification professionnelle; quant au SG DDPS, il réalise *Cyber Pakt*, un exercice unique en Suisse, avec lequel il entraîne les moyens du DDPS en y invitant les partenaires des autres départements et les opérateurs d'infrastructures critiques importants pour lui.

Capacités opérationnelles techniques: une fois les objectifs atteints, le DDPS disposera d'environ 150[8] collaborateurs. Ces moyens seront renforcés en terme de compétences et de capacité à durer par 400 à 600 militaires, un effectif qui sera atteint d'ici 6 à 7 ans. Les comparaisons sont toujours aléatoires, mais pour se situer on citera le 13ème rang sur 22 atteint par le *team* aligné à *Locked Shield 2018* et dont la progression qualitative depuis 2017 a été significative.

Développement et anticipation: avec armasuisse Sciences et Technologie le DDPS dispose d'une « mini-DARPA »[9] avec des liens bien établis avec les milieux de la recherche et avec des projets concrets; le projet CYD-Campus (campus cyberdéfense) dotera ensuite le DDPS d'un réseau agile pour le renforcer en matière de compétences et de capacités.

Défis

Le nombre de variables et d'inconnues étant important et évolutif, il ne permet pas d'établir des pronostiques précis. La réalisation du PACD c'est donc avant tout de la conduite[10] où il faut jongler avec la pénurie de spécialistes, les dimensions du problème, un état des lieux lacunaire, sans cesse de nouvelles vulnérabilités, mais aussi de nombreuses initiatives privées et publiques. Et le PACD doit être réalisé sans mettre en danger la réforme en cours de l'armée (DEVA) ni le projet Air 2030, vital pour rénover la défense aérienne. Le Plan d'action cyberdéfense du DDPS n'est donc pas un aboutissement; il n'est qu'une première feuille de route permettant au DDPS de s'adapter aux défis d'un cyberespace devenu enjeu majeur de la politique de sécurité et qui ne peut pas attendre. L'absence d'attaques majeures jusqu'ici ne saurait en effet être une excuse pour reporter nos efforts, car les acteurs mal intentionnés profitent déjà de nos lacunes et pourraient, en cas de conflit nous infliger des dégâts insupportables.

G. V.

7 Conduit par le *Cooperative Cyber Defence Center of Excellence* de Tallinn (Estonie).

8 Ces chiffres sont à considérer comme «nets» car très peu de postes sont «mangés» par des tâches administratives, d'infrastructure ou de sécurité, celles-ci étant fournies par les organisations de base déjà en place.

9 La *Defense Advanced Research Projects Agency* est l'agence du US DoD chargée de la recherche et du développement des nouvelles technologies à usage militaire.

10 Un rapport de situation et une conférence au niveau départemental sont à cet effet réalisés chaque trimestre.