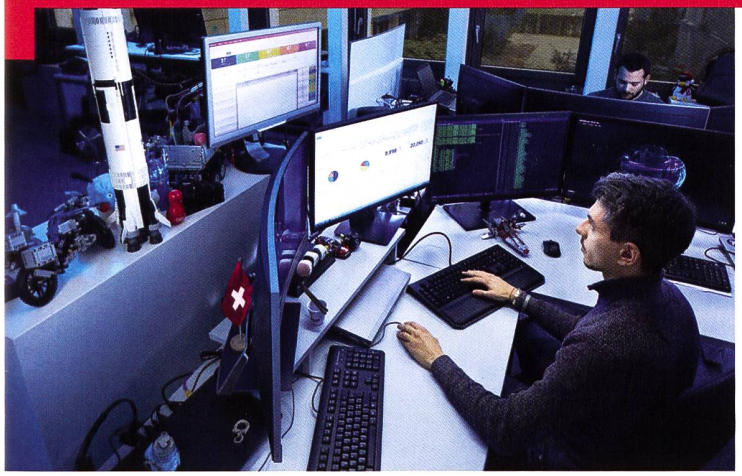
La sécurité informatique est un processus et non pas un état



L'Armée suisse dispose actuellement d'une infrastructure TIC (technologies de l'information et de la communication) hétérogène qui s'est développée au fil du temps. Certaines technologies encore utilisées de nos jours remontent à plusieurs décennies, tandis que le progrès technologique avance à un rythme effréné. Cette situation confronte la sécurité informatique à de grands défis, le fonctionnement et la sécurité de certains systèmes étant souvent en contradiction. Afin de remettre toutes ces infrastructures hétérogènes à niveau, des modifications fondamentales ont été décidées et entreprises ces dernières années pour moderniser l'informatique militaire.

Cyberdéfense

La sécurité informatique est un processus et non pas un état

Anna Muser

Cheffe communication Base d'aide au commandement (BAC)

Article reproduit avec l'aimable autorisation de la Communication Défense

Au printemps 2018, l'ancien chef de la Base d'aide au commandement (BAC) a lancé un projet interne visant à accroître la sécurité des systèmes TIC de l'Armée suisse. L'élément déclencheur a été un incident lié à la cybersécurité qui s'est produit chez RUAG, mais aussi la découverte de failles dans les systèmes TIC de l'armée suite à des rapports, des tests et des essais d'intrusion. Des analyses toujours plus poussées ont révélé l'urgente nécessité d'agir. La mise en œuvre du projet se terminera dans un avenir proche. Cependant, afin de mettre en lumière le contexte actuel, un retour en arrière s'impose.

L'histoire de la BAC

L'actuelle BAC existe en l'état depuis 2005. À l'époque, le Groupe de l'aide au commandement (Gr aide cdmt) a fusionné avec la Direction de l'informatique et de la communication (Dir infm DDPS). C'est aussi à cette époque que les systèmes informatiques militaire et civil du DDPS ont été fortement imbriqués. Les deux domaines avaient jusqu'alors poursuivi des objectifs totalement différents ; le personnel de ces entités avait des conceptions différentes de la sécurité, et les tâches à accomplir dans ces systèmes cloisonnés étaient difficilement conciliables. C'est à la fusion du Gr aide cdmt et de la Dir infm DDPS que l'on doit le fait que la BAC fournit aujourd'hui des prestations aussi bien pour le compte de l'armée et du Réseau national de sécurité (RNS) que de l'administration fédérale civile (DDPS ou autres départements).

En avril 2016, suite à l'incident survenu chez RUAG, Guy Parmelin, ancien chef du DDPS, a décidé de dissocier de nouveau les systèmes informatiques de l'armée et de l'administration. C'était là le seul moyen pour la BAC d'avoir une chance de parvenir à maîtriser des défis tels que l'adaptation au progrès technologique effréné, aux menaces croissantes dans le cyberespace et aux besoins de plus en plus importants de l'armée et de se concentrer sur sa mission de base.

Dissociation de l'informatique civile et militaire

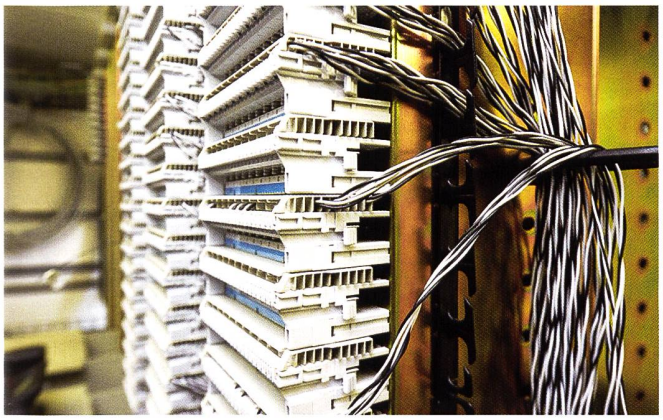
Dans le cadre du programme de dissociation des prestations informatiques de base, les systèmes de l'armée et du RNS revêtant une importance décisive pour l'engagement et posant des exigences élevées en termes de sécurité et de robustesse sont dûment séparés des systèmes de l'administration fédérale et fonctionneront, à l'avenir, de façon totalement autonome et distincte des systèmes civils. Le concept de dissociation prévoit que les systèmes militaires puissent échanger des informations de manière sûre et contrôlée avec le reste de l'administration fédérale et le monde civil. La dissociation des prestations informatiques de base et la création des nouvelles zones présentent trois avantages majeurs :

- La sécurité informatique des systèmes revêtant une importance décisive pour l'engagement sera considérablement accrue ;
- Les responsabilités pour la sécurité informatique seront clairement définies dans les différentes zones ;
- La BAC pourra se concentrer pleinement sur la fourniture de prestations pour l'armée et le RNS.

La fourniture des prestations de base, qui comprennent des dizaines d'application spécialisées civiles, devrait être déléguée au terme de la dissociation. Ainsi, l'ensemble de la bureautique pour quelque 15'000 utilisateurs sera transférée à l'Office fédéral de l'informatique et de la télécommunication (OFIT). Grâce aux économies d'échelle, les coûts informatiques pour l'administration seront réduits. Cette séparation des systèmes a déjà été réalisée depuis longtemps pour l'environnement hautement sécurisé du Centre des opérations électroniques, qui fournit des prestations dans le cyberespace et l'espace électromagnétique.

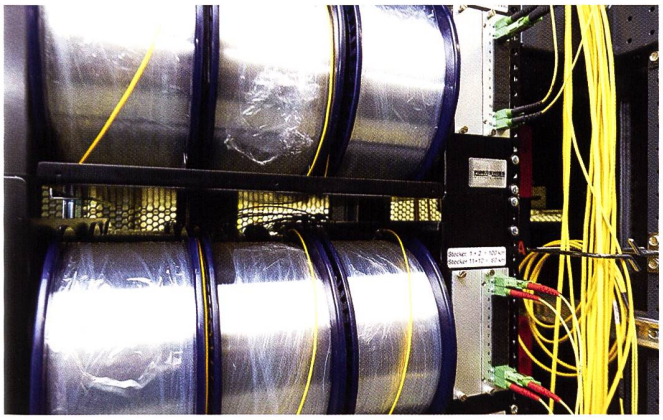
Vers un système entièrement neuf

Afin de pouvoir réaliser la dissociation, une autre décision de principe était nécessaire. Soit l'on choisissait



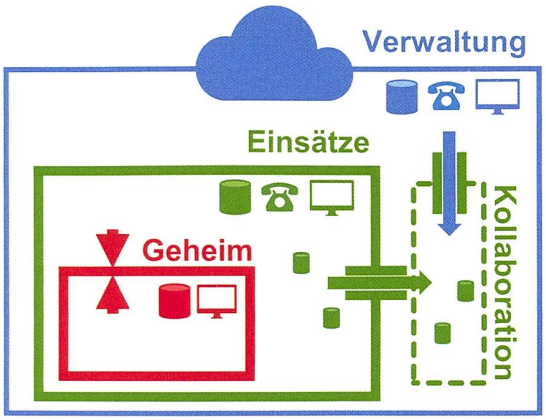
Dans l'environnement de test du Réseau de conduite suisse, le contexte précédant la transition vers un système entièrement neuf est bien visible. Des câbles datant des années 1950 ... (© VBS/DDPS, photos: CME)

...cohabitent avec de la fibre optique moderne au sein de l'environnement informatique de l'Armée suisse.



de continuer d'utiliser les anciens systèmes pendant la dissociation, ce qui serait revenu à pratiquer une opération à cœur ouvert, soit l'on créait, parallèlement aux systèmes actuels, un système entièrement nouveau. En raison de la complexité de l'opération et des ressources disponibles, la deuxième solution a été retenue. L'ancien environnement informatique hétérogène sera donc abandonné pour laisser place à un système entièrement neuf.

De manière schématique, les différentes prestations informatiques au sein du DDPS sont décomposées en zones soumises à divers critères.

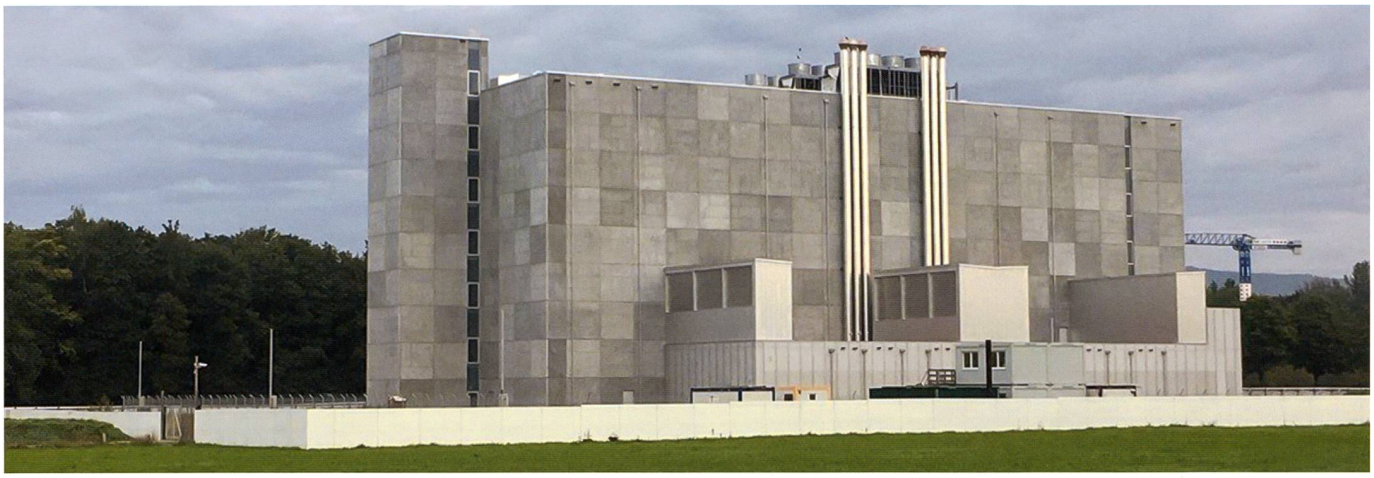


A cet égard, les prestations rassemblées dans le programme FITANIA constituent les fondements nécessaires. Avec l'adjudication du marché à Swisscom à l'automne 2019 pour la création de la plateforme des nouveaux centres de calcul, un partenaire industriel adéquat a été trouvé. Une approche moderne de la sécurité sera mise en œuvre d'emblée dans la nouvelle infrastructure informatique, ce qui permettra de garder constamment une vue d'ensemble des actifs informatiques et de garantir la continuité des services informatiques. Dans ce contexte, ce ne sont plus des systèmes individuels qui seront protégés, mais plutôt des informations. Certains systèmes anciens encore utilisés aujourd'hui mais qui ne satisfont plus aux exigences de sécurité actuelles ont déjà été isolés comme il se doit. Une extension de la protection informatique à des systèmes obsolètes ne serait pas viable économiquement. L'une des conséquences de cette façon de procéder est que les risques liés à ces systèmes isolés obsolètes sont sciemment supportés par le DDPS. De cette façon, les différences de ces systèmes vis-à-vis des principes de protection de base de la Confédération ne sont pas rapportées à l'Unité de pilotage informatique de la Confédération (UPIC), pourvu qu'elles ne mettent pas en péril les systèmes informatiques de la Confédération. Une annonce à l'UPIC aurait, en soi, entraîné des risques de sécurité.

La question de la gouvernance

L'ordonnance sur l'informatique dans l'administration fédérale (OIAF) règle la gouvernance informatique dans l'administration fédérale, l'UPIC étant l'organe compétent dans ce domaine. Le Contrôle fédéral des finances (CDF) réalise les audits et maintient une vue d'ensemble des systèmes informatiques. Les différentes applications fournies par la BAC doivent toutefois satisfaire à des exigences de sécurité particulièrement élevées. Ainsi par exemple, les directives de sécurité des systèmes militaires sont très complètes, notamment dans les domaines de la protection et de la défense contre les menaces du cyberespace. La sécurité des systèmes militaires doit donc être vérifiée en utilisant un catalogue de critères étendu. À cette fin, un système de gestion de la sécurité de l'information (*Information Security Management System*, ISMS) spécifique a été mis en place à la BAC. Fin 2018, l'ISMS de la BAC a reçu la certification ISO/IEC 27001 de la SQS.

Grâce à la mise en œuvre conséquente de la dissociation, le DDPS assume d'ores et déjà la responsabilité de ses propres systèmes ainsi que les risques en résultant. Les directives de l'UPIC relatives aux principes de protection de base de la Confédération sont ainsi dûment appliquées, voire renforcées si nécessaire. Dans certains cas, il est néanmoins tout à fait possible que ces directives ne puissent être respectées pour les systèmes militaires, et ce pour des raisons techniques. Par exemple, l'authentification à deux facteurs ne peut pas être intégrée sur d'anciens systèmes produits par des fabricants tiers.



Le centre de calcul de Frauenfeld est l'un des éléments visibles du programme FITANIA, avec lequel la future infrastructure numérique de l'armée sera réalisée.

En plein processus

En raison de la complexité des systèmes existants, il est impossible de mettre en place du jour au lendemain un environnement informatique robuste et hautement sécurisé pour l'Armée suisse. Les processus d'acquisition de l'administration fédérale, les ressources disponibles et les exigences auxquelles la BAC est actuellement soumise ont une influence notable sur le calendrier de mise en œuvre. Depuis 2018 et sa réorientation stratégique, la BAC tout entière se mobilise pour fournir des prestations informatiques et des opérations électroniques robustes et hautement sécurisées en toutes circonstances au bénéfice de l'Armée suisse. Afin d'identifier le niveau de sécurité dans la transformation en cours, plusieurs tests ont été réalisés à l'été 2018 avec des partenaires issus de l'industrie. Les résultats obtenus ont déjà permis d'augmenter considérablement la sécurité contre d'éventuelles manipulations indésirables et intrusions. De plus, un nouveau projet visant à automatiser la configuration des pare-feu a été lancé. De cette manière, les facteurs d'erreur humains ont pu être réduits au strict minimum, et l'état des différents composants peut être contrôlé facilement en tout temps.

De nouvelles directives de sécurité architectoniques s'appliquent désormais aux systèmes existants; ces directives seront également appliquées aux futurs projets. A cet égard, une nouvelle structuration des systèmes de logiciels et des plateformes sur lesquelles ceux-ci reposent a été mise en place. L'une des mesures phare est la création du domaine Cyber Security et du poste de chef Cyber Security (CISO BAC). Les forces de sécurité de la BAC sont désormais concentrées dans ce nouveau domaine, qui regroupe les sections Stratégie de sécurité et Sécurité intégrale, ainsi que le Cyber Fusion Center. Ce dernier rassemble toutes les informations issues du cyberespace afin d'accroître le contrôle de la sécurité. Ceci permet en effet d'augmenter la surveillance des activités réseau. Une équipe Formation et *awareness* en matière de cybersécurité a été créée spécialement pour former les collaborateurs internes et externes de la BAC; cette équipe gère des modules d'apprentissage en ligne ainsi que des formations physiques afin d'accroître la sécurité. Par ailleurs, depuis le début de 2020, la BAC dispose aussi de l'*ICT Warrior Academy*, où des spécialistes sont formés aux nouvelles exigences de l'armée et reçoivent de nouvelles compétences. Dans le domaine Renouvellement, des méthodes agiles sont développées pour accroître la transparence, réagir plus rapidement aux exigences des clients et intégrer précocement les dernières technologies. En outre, en se concentrant sur la dissociation et la finalisation de FITANIA, des éléments garantissant une importante amélioration de la sécurité informatique seront mis en place au cours des prochaines années.

Développement du commandement Cyber

Il s'agira dorénavant de pouvoir utiliser les moyens de l'armée avec précision en s'appuyant sur une avancée des connaissances et en anticipant les décisions. C'est pourquoi un réseau numérique souple formé de capteurs et d'effecteurs est nécessaire, permettant au commandant de prendre plus rapidement les bonnes décisions. Les capacités dans ce domaine doivent être encore davantage regroupées pour faire face aux menaces de plus en plus élevées, tant quantitativement que qualitativement. Dans le cadre de la motion Dittli de mars 2018, le Parlement a demandé le développement de la BAC en un commandement Cyber. Il s'agit en outre de la suite logique du développement de la BAC dans le cadre des objectifs 2030+ de l'Armée suisse. Le projet est actuellement dans sa phase d'initialisation, et une adaptation nécessaire de la loi sur l'armée est prévue. Afin de pouvoir garantir des prestations informatiques et des opérations électroniques robustes et hautement sécurisées en toutes circonstances au bénéfice de l'armée, la BAC a avant tout besoin de conditions stables et d'une endurance à toute épreuve.

A. M.