Le "Cyber 9/12 Strategy Challange" : une simulation de crise digitale pour les experts de cyber-securité de demain

Autor(en): **Dewar, Robert S.**

Objekttyp: **Article**

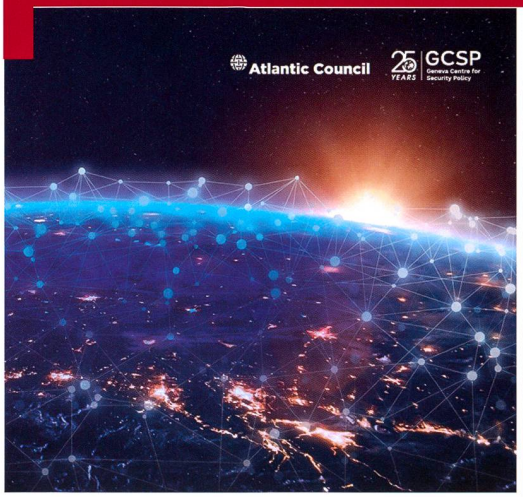
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2020)**

Heft 6

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-913940



Le Centre de politique de sécurité, Genève (GCSP) est un centre de formation international dédié aux questions de sécurité. Fondation internationale comptant 45 Etats membres, le centre offre des cours pour des décideurs d'administrations nationales et du secteur privé et associatif. Par la recherche et l'organisation de conférences, le GCSP favorise la réflexion et le dialogue sur les grands thèmes de sécurité internationale.

Cyberdéfense

Le « Cyber 9/12 Strategy Challenge » – Une simulation de crise digitale pour les experts de cyber-securité de demain

Dr. Robert S. Dewar

Head of Cyber Security and Director of the Cyber 9/12 Strategy Challenge (Geneva), Geneva Centre for Security Policy

Cette année, le Centre de Politique de Sécurité de Genève (GCSP) célèbre son 25e anniversaire. Les 2 et 3 juillet 2020, le GCSP a accueilli la 6e édition de l'étape genevoise du Cyber 9/12 Strategy Challenge. Organisé en partenariat avec l'Atlantic Council (AC), le GCSP a accueilli des étudiants du monde entier, notamment de Suisse, d'Estonie, du Royaume-Uni, de Finlande, Norvège, France, des Etats-Unis et d'Inde. Vingt équipes se sont affrontées pour être couronnés champions de la compétition. attribuée à l'équipe PromETHeus de l'ETH Zurich, après un round final entièrement disputé par des équipes de l'ETH ! Le premier prix a été annoncé et décerné par S.E. M. Andrew Bremberg, représentant permanent des Etats-Unis d'Amérique auprès de l'Office des Nations Unies et des autres organisations internationales à Genève, et l'ambassadeur Christian Dussey, directeur du GCSP.

Cette année, la compétition a accueilli pour la première fois une équipe d'Inde. C'est aussi la première fois que l'événement s'est déroulé entièrement virtuellement, en utilisant des plateformes de conférence en ligne pour permettre aux participants de participer depuis n'importe où dans le monde.

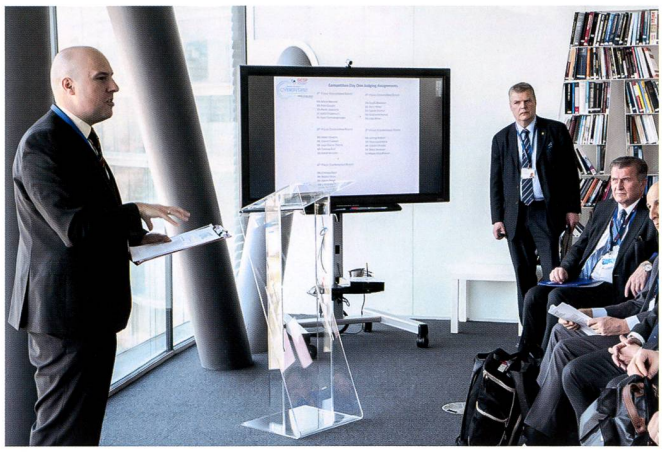
Contexte de la Competition

Le Cyber 9/12 Strategy Challenge est une série de compétitions annuelles de développement de recommandations po-litiques et stratégiques organisées dans le monde entier. Les compétitions mettent les participants au défi de créer des solutions et des recommandations politiques innovantes en réponse à un incident de cybersécurité fictif et évolutif. Cette année, les équipes devaient faire face à une crise affectant l'approvisionnement des infrastructures énergétiques essentielles d'un un pays fictif. Aux premiers abords, le *scénario* laissai entendre que l'incident pourrait avoir été commandité par un Etat. Au fur et à mesure que le scénario se développait, le cyber-incident fictif semblait en effet être un prélude à une invasion. Il s'avère ensuite que l'incident résulte de l'acte d'un seul employé mécontent qui avait récemment été licencié. Des équipes prenant part dans la compétition ont dû donc faire face à la complexité liée au fait d'avoir d'abord recommandé des politiques militaires pour ensuite devoir désamorcer la situation pour éviter un conflit.

Le Cyber 9/12 Strategy Challenge est une serie de compétition rendue unique précisément grâce à l'accent mis sur le développement de recommandations politiques et stratégiques. Il existe en effet de nombreux événement se focalisant sur la partie technique de la cybersécurité. On pense notamment au « Hackathons ». En revanche, le Cyber 9/12 Strategy Challenge est spécifiquement conçu pour le développement et l'étude de solutions politiques et géostratégiques. Il n'est pas nécessaire d'avoir une formation technique pour y participer.

La série des Cyber 9/12 Strategy Challenge est coordonnée par l'Atlantic Council, basé à Washington, D.C. Créé en 2012 par Jason Healey alors qu'il était directeur de la Cyber Statecraft Initiative au Atlantic Council, le Challenge a été conçu dès le départ comme un événement destiné aux étudiants. Toute personne inscrite à un cours universitaire peut y participer.

Alors que la compétition initiale était un événement annuel unique destiné aux étudiants américains, le Challenge s'est développé au fur et à mesure des années, et englobe aujourd'hui sept événements indépendants dans le monde entier. Les Cyber 9/12 Strategy Challenges se déroulent maintenant à Londres (Royaume-Uni), Lille (France), Genève (Suisse) et Canberra (Australie) ainsi que des compétitions américaines à Austin (Texas), New York et Washington. Cela a créé une « saison » 9/12, avec tous les concours se déroulant au cours de l'année civile universitaire de septembre à mai, afin de garantir que tous les étudiants bénéficient du plus grand soutien de leur faculté.



Briefing des juges du Cyber 9/12 Strategy Challenge.

Les juges du Cyber 9/12 Strategy Challenge écoutent une présentation du concours.

Qui soutient la compétition ?

Depuis sa création, la compétition repose sur le soutien du secteur public et du secteur privé. Toutefois, au fil des années, le niveau d'engagement a augmenté de manière exponentielle. Parmi les entreprises qui le parrainent et le soutiennent, on trouve de grands conglomérats internationaux tels que Facebook, Kudelski, KPMG et FireEye.

La compétition a également bénéficié d'un soutien important des gouvernements du Royaume-Uni, de la Finlande, de l'Estonie, de l'Australie, de la France et de la Suisse. Pour la compétition de 2020, nous avons accueilli le soutien de la Mission des Etats-Unis à Genève.

Comment la compétition se déroule-t-elle ?

Sur deux jours, la compétition exige des participants qu'ils réagissent à un incident de cyber sécurité de plus en plus grave.
Les incidents abordés dans le cadre des compétitions sont nombreux et variés. A ce jour, ils ont porté sur des questions aussi diverses que le piratage des systèmes de contrôle du trafic aérien, les défaillances systémiques des réseaux de navigation maritime et de contrôle des autorités portuaires, l'exploitation des capacités militaires de commandement et de contrôle ou les opérations de rançon contre des entreprises civiles de télécommunications. Ces incidents fictifs sont d'abord localisés, mais ils ont un impact et une ampleur suffisants pour justifier une enquête par un groupe de travail (fictif) composé de représentants des États membres européens.
Dans les semaines avant la compétition, les équipes reçoivent un « Intelligence Brief ». Il s'agit d'un ensemble d'articles de presse, de rapports officiels, de dossiers de renseignements et de publications sur les réseaux sociaux - tous entièrement fictifs - contenant des détails sur l'incident. Une fois sur place, le premier jour de la compétition, toutes les équipes présentent leurs recommandations en réponse aux informations contenues dans le dossier de renseignement à un jury. Les juges jouent le rôle des chefs d'Etat et de gouvernements convoqués pour traiter de la crise.

Les équipes sont tenues de présenter des options politiques pour faire face a la crise, et de faire une recommandation. Elles sont jugées non seulement sur leurs compétences en matière de présentation, mais aussi sur leur compréhension de la situation, leur maîtrise de la politique de cybersécurité et leur compréhension du contexte géopolitique dans lequel l'incident fictif se déroule. Non seulement les juges défient les concurrents en demandant des justifications pour leurs recommandations politiques, mais ils fournissent également un retour sur ces recommandations d'un point de vue professionnel et réel. Ces juges attribuent des points pour les présentations, les équipes ayant obtenu les meilleurs scores accédant à la demi-finale le matin du deuxième jour.

Le soir du premier jour, les équipes qui sont avancées aux demi-finales reçoivent un deuxième « Intelligence Brief » décrivant une intensification de la crise et travaillent toute la nuit afin de préparer leur présentation pour la demi-finale. Cela implique souvent que les équipes travaillent toute la nuit sur leur recommandation !

Lors des demi-finales, les équipes présentent à nouveau devant un panel d'experts, et quatre équipes sont sélectionnées pour participer à la finale. En finale, les équipes reçoivent le troisième et dernier « Intelligence Brief » décrivant une nouvelle intensification de la crise et disposent de 30 minutes pour préparer leurs réponses avant de présenter pour la dernière fois devant un panel d'experts.

Les équipes

Pour participer au Cyber 9/12 Strategy Challenge en tant que concurrent, les participants doivent être inscrits à un cours universitaire au moment de l'inscription. Les équipes sont souvent constitués d'étudiants de niveau Bachelor, ainsi que de Mater et de Doctorat.

Etre inscrit à un programme universitaire scientifique ou informatique n'est pas requis pour participer à la compétition. Au contraire, nous encourageons la participation d'étudiants de sciences politiques, pour apporter une manière de penser nouvelle et innovante a

Les équipes se préparent à participer au Cyber 9/12 Strategy Challenge.

des problèmes techniques. Nous permettons ainsi une interaction directe entre la politique sociale et l'expertise technique. Ce mélange aide les législateurs, les décideurs politiques et les dirigeants de demain à aborder la cybersécurité et la politique digitale avec une perspective plus globale, en encourageant des solutions plus créatives. Le Cyber 9/12 Strategy Challenge est un « sport d'équipe ». Les participants ne peuvent donc pas y prendre parts tout seules, mais doivent faire partie d'une équipe de 4. Il est aussi nécessaire d'avoir un coach. Les coaches peuvent être des professeurs d'université, professionnels de l'informatique, anciens fonctionnaires. Leur rôle est de guider les équipes dans les phases de préparation et de compétition. Pour éviter de donner un avantage aux participants provenant d'institutions avec plus de ressources, les équipes ne peuvent que constater leur coach durant la compétition. Recevoir de l 'aide extérieur est interdit.

Les équipes viennent du monde entier pour participer. Les participants réguliers à la compétition de Genève sont l'Université de Saint-Gall, l'ETH Zurich, l'EPFL Lausanne, U.S Military Academy at West Point et le U.S Naval College des États-Unis et l'Université de Glasgow. Cette diversité de participation est retrouvée dans la diversité des solutions présentés durant la compétition, du fait des différents contextes culturels et régionaux des différentes équipes.

Comment la compétition est-elle jugée ?

Les juges sont tout aussi importants pour la compétition que les participants eux-mêmes. Les juges des sept événements annuels de Cyber 9/12 sont issus de nombreux horizons. Ils sont des représentants du monde universitaire, des diplomates actuels et anciens, des fonctionnaires de carrière travaillant dans des organisations nationales et régionales, des professionnels du secteur de la cybersécurité et des représentants de la société civile. Tous ont une grande expérience de la cybersécurité. Ils donnent de leur temps et mettent leur expertise et leur expérience au service de la compétition afin de juger les réponses des participants mais aussi de donner un aperçu des processus décisionnels réels. De nombreux juges ont été appelés à proposer des options politiques dans des cybercrises réelles et connaissent bien les processus politiques et juridiques complexes nécessaires pour réagir de manière efficace et opportune à une crise.

Cette interaction entre les étudiants et les professionnels de la cyber-sécurité est vitale car elle aide les participants à faire la différence entre la fiction, et la réalité de la gestion nationale, régionale et mondiale de la cybersécurité. Cette expérience permet d'informer les futurs dirigeants sur les réalités et les aspects pratiques de la conception de solutions politiques de cybersécurité, ou sur les cadres juridiques, réglementaires et civiques dans lesquels les gouvernements, l'industrie et la société doivent opérer. Une telle expérience est cruciale pour un monde numérique plus sûr.

De plus...

Le Cyber 9/12 Strategy Challenge n'est pas seulement l'occasion pour les élèves de se mesurer à une cyber-crise en pleine évolution. C'est aussi une occasion inestimable de « networking » pour les participants et les juges. En plus de la compétition, des événements parallèles tels que des séances d'orientation professionnelle, des panels de haut niveau discutant des derniers développements géopolitiques, des discours en plénière et des ateliers ont lieu. Ces derniers servent à créer une communauté de professionnels et d'experts afin d'avoir le plus grand impact possible sur le monde numérique d'aujourd'hui.

Ces occasions pour les étudiants s de rencontrer et d'interagir avec des professionnels et des experts de haut niveau issus des mondes techniques et politiques sont inestimables et peuvent fournir des informations utiles aux étudiants dans leurs domaines de prédilection. Elles permettent également aux juges de rencontrer la prochaine génération de talents dans le domaine de la cybersécurité. Un certain nombre de concurrents proches de la fin de leurs études ont obtenu des stages et des contrats de travail grâce aux contacts établis lors du Challenge.

L'impact du COVID-19 sur la compétition 2020 à Genève

En 2020, le Cyber 9/12 Strategy Challenge a pris une tournure inattendue. Dans des circonstances normales, le GCSP accueille plus de 300 personnes à la Maison de la paix pendant deux jours de séminaires, de concours, de discussions, de plénières et de séances de networking. La pandémie mondiale de COVID-19 a fait que la compétition normale ne pouvait pas se dérouler en toute sécurité.

En discussion avec nos partenaires de L'Atlantic Council, le GSCP a choisi d'organiser une compétition virtuelle. Tirant parti de notre propre expérience croissante dans l'organisation de grands événements en ligne et de celle de L'Atlantic Council qui a organisé une compétition virtuelle plus tôt dans l'année à Washington DC, le GCSP a converti le format du Challenge en une expérience entièrement en ligne. Les équipes ont présenté leurs recommandations aux juges par vidéoconférence depuis le monde entier, et les sessions plénières, les discours et les événements parallèles ont tous été organisés en ligne.

La conversion numérique a été bien accueillie par les participants et les juges. Bien que les possibilités de réseautage aient été limitées en raison du manque d'interaction physique, les sessions du Challenge elles-mêmes, ainsi que la série d'événements parallèles proposés, ont permis aux élèves de continuer à participer, à s'engager et à discuter des derniers développements cybernétiques avec les juges. Un panel de haut niveau impliquant S.E. M. Andrew Bremberg (représentant permanent des Etats-Unis d'Amérique auprès de l'Office des Nations unies et d'autres organisations internationales à Genève), Mme Chelsey Slack (chef adjoint de la cyberdéfense, OTAN), le Dr Trey Herr (directeur de la Cyber Statecraft Initiative, Atlantic Council) et animé par le Dr Robert Dewar (chef de la cyber sécurité au GCSP et directeur du Geneva Cyber 9/12 Strategy Challenge) a réuni plus de 100 participants virtuels et a donné lieu à une discussion intéressante sur les derniers développements de la cyber diplomatie.

Le succès de la logistique considérable qu'a impliqué la coordination de plus de 200 appels individuels en ligne pendant deux jours témoigne du dévouement et du travail acharné de l'équipe du Cyber 9/12 du GCSP, ainsi que de l'agilité du GCSP à s'adapter à des événements soudains, inattendus et extrêmement importants. À la suite de ces expériences, le GCSP et le Atlantic Council apportent leur soutien à d'autres événements Cyber 9/12 dans le monde entier qui envisagent également de passer au format numérique. L'une des leçons tirées de cette conversion est qu'elle a ouvert la porte à la participation d'un plus grand nombre d'étudiants de pays plus lointains, et pas seulement du monde occidental. Ces compétitions deviennent de véritables affaires mondiales.

Qu'est-ce que le Cyber 9/12 Strategy Challenge apporte-t-il à la Suisse ?

Les équipes des universités suisses ont toujours été des concurrents réguliers du Cyber 9/12 de Genève, et ont historiquement obtenu de très bons résultats. Cette année, cependant, la représentation suisse a connu une année exceptionnelle face à une forte cohorte internationale. Les équipes de l'ETH Zurich ont pris les cinq premières places du classement. L'expérience des institutions universitaires suisses s'est développée ces dernières années pour comprendre non seulement l'interrelation entre la politique de cybersécurité et les solutions techniques, mais aussi comment placer ces solutions dans un contexte géopolitique et géostratégique plus large. La plupart des étudiants des équipes des institutions suisses, mais pas tous, sont eux-mêmes suisses. Ils sont les futurs experts, législateurs et dirigeants de la Suisse en matière de cybersécurité. En participant au Cyber 9/12 et en faisant face à des équipes du monde entier ils élargissent leur base de connaissances et leur expérience, ce qui leur permettra d'élargir leur perspective au-delà des processus européens de résolution de problèmes. Les défis auxquels nous sommes confrontés aujourd'hui ne nous sont pas propres. Mais en apprenant comment d'autres parties du monde font face à ces mêmes défis, les futurs experts suisses aborderont ces défis de manière nouvelle et créative.

La tenue de l'un des sept défis à Genève renforce également la position internationale de la Suisse en tant que centre de *leadership* créatif dans le domaine de la cybersécurité. La Genève internationale est déjà un centre dynamique pour la politique numérique. Mais le Cyber 9/12 Strategy Challenge sert de point de rencontre - un lien - pour les experts et professionnels techniques, juridiques, sociaux et politiques. C'est l'occasion de rencontrer et de dialoguer avec des représentants de tous les secteurs nécessaires à la réalisation d'un monde plus sûr sur le plan numérique. L'itération genevoise de la compétition bénéficie déjà d'un excellent soutien de la part du gouvernement suisse, mais nous espérons que ce soutien se poursuivra et s'élargira.

Le Cyber 9/12 Strategy Challenge est un investissement unique dans l'avenir de la Suisse, à la fois en termes de soutien aux jeunes qui y participent, mais aussi en termes de facilitation du partage d'idées et d'expériences entre les professionnels de première ligne actuels et anciens. Le Challenge a donc un impact significatif sur l'élaboration des politiques internationales en matière de cybersécurité dans de nombreux domaines. En raison de la diversité des thèmes abordés dans les scénarios - de la sécurité aérienne à la sécurité maritime en passant par l'approvisionnement en énergie -, il a un impact sur l'élaboration de la politique de cybersécurité dans toute une série de domaines politiques. Les professionnels qui jugent les équipes

considèrent le Challenge comme un banc d'essai pour des solutions créatives à certains des défis les plus complexes auxquels nous sommes confrontés aujourd'hui en matière de cybersécurité. Le Challenge n'est donc pas un simple concours d'étudiants : c'est un centre de réflexion créative et d'élaboration de solutions.

Conclusion

Au fil des ans, le Cyber 9/12 Strategy Challenge de Genève a pris de l'ampleur et s'est heurté à des obstacles logistiques uniques. Cette année, le COVID-19 a obligé les organisateurs à se lancer dans l'inconnu et à organiser une compétition internationale de grande envergure totalement en ligne. Les évènements en ligne semblent destinés à faire partie de la vie quotidienne pendant un certain temps encore. Nous allons donc nous adapter à cette nouvelle normalité et espérons étendre la participation au Challenge encore plus loin. Nous attendons avec impatience ce que 2021 nous apportera.

R. D.

Liens :
Cyber 9/12 Strategy Challenge in Geneva, Switzerland
Atlantic Council Cyber 9/12 Strategy Challenge homepage

News

Renforcement de la cyberdéfense

Berne, 07.10.2020 – Lors de sa séance du 7 octobre 2020, le Conseil fédéral a lancé la procédure de consultation portant sur diverses modifications touchant la loi sur l'armée, l'organisation de l'armée et d'autres bases légales. Il entend notamment créer un commandement Cyber et accroître les effectifs de milice dans ce domaine. Parmi les autres nouveautés notables, la mise en place d'une nouvelle autorité responsable du trafic aérien militaire pour assurer la sécurité des Forces aériennes ainsi qu'un renforcement de l'appui aux événements civils. La consultation prendra fin le 22 janvier 2021.

La mise en œuvre du processus développement de l'armée (DEVA) a débuté le 1er janvier 2018 et se terminera le 31 décembre 2022. D'emblée, il s'est avéré que des adaptations étaient nécessaires dans divers domaines, malgré les mesures internes de correction que l'armée a déjà prises et appliquées, pour partie. Certains de ces domaines exigent que la loi sur l'armée (LAAM), l'organisation de l'armée (OOrgA) et d'autres bases légales soient révisées.

La Base d'aide au commandement deviendra le commandement Cyber en 2024

En concrétisant le DEVA, il était prévu de subdiviser l'armée en trois domaines distincts : le commandement des Opérations, le commandement de l'Instruction et le commandement du Soutien, lui-même composé de la Base d'aide au commandement (BAC) et de la Base logistique de l'armée (BLA). En application de la motion 19.3427, que les Chambres fédérales ont adoptée lors de la session d'été 2020, décision a été prise de renoncer, dans le cadre de la révision LAAM/OOrgA, à mettre la BAC et la BLA sous un même commandement car il n'en résulte aucune possibilité d'optimisation par rapport à l'organisation actuelle.

Vu les menaces qui prédominent actuellement, le Conseil fédéral entend transformer la BAC en un commandement spécifique appelé commandement Cyber au début de 2024, ce qui nécessite une adaptation de l'OOrgA. La numérisation ainsi que la modernisation et la mise en réseau qui en résulteront de tous les systèmes de l'administration militaire et de l'armée progressent rapidement. Cette évolution soumet une architecture informatique uniformisée à de fortes exigences et exige une standardisation des applications. De plus, les processus croissants de mise en réseau augmentent sensiblement le nombre de défis à relever dans le domaine de la cyberprotection. Aussi, pour faire face du mieux possible à ces exigences, la BAC devra se transformer pour passer d'une organisation de soutien largement sectorisée à un commandement militaire strictement opérationnel.

Le commandement Cyber devra organiser les capacités militaires clés dans les domaines de l'image de la situation, de la cyberdéfense, des prestations informatiques, de l'aide au commandement, de la cryptologie et de la guerre électronique.

Cyberinstruction à l'armée complétée en coopérant avec des externes

Au niveau de l'armée également, il est prévu d'augmenter ces prochaines années l'effectif du personnel dans le domaine de la cyberdéfense avec la mise sur pied, le 1er janvier 2022, d'un cyberbataillon et d'un état-major spécialisé correspondant, faisant ainsi passer l'effectif actuel du personnel de milice, qui est de 206, à 575 militaires. Pour accroître également la qualité de l'instruction dispensée à ces cyberspécialistes au sein de l'armée, celle-ci sera complétée par un stage auprès de partenaires externes, permettant ainsi d'approfondir et d'étendre les capacités acquises et, au final, d'en faire bénéficier l'armée.

Création d'une autorité du trafic aérien militaire et autres adaptations

Jusqu'à présent, la Suisse ne dispose pas d'organisation comparable à l'Office fédéral de l'aviation civile pour le trafic aérien militaire. Des bases légales vont donc être créées pour une autorité du trafic aérien militaire. Celle-ci doit assurer la sécurité des Forces aériennes lors de leurs missions dans l'espace qu'elles partagent avec l'aviation civile. Elle veillera notamment à éviter tout incident ou accident dans cet espace et à garantir mieux encore la surveillance et la régulation du trafic aérien militaire. Une adaptation de la loi sur l'aviation s'impose donc.
Appui renforcé aux événements civils

Dans la foulée de la révision de la LAAM, le Conseil fédéral entend aussi renforcer l'appui apporté par l'armée aux événements civils. Cela commencera par un accroissement de la souplesse et des disponibilités de l'armée dans le sens où les recrues en phase d'instruction de base pourront, elles aussi, être engagées, et plus seulement les militaires en service long et ceux en cours de répétition. L'armée devra également pouvoir fournir des prestations dans un cadre limité lors d'événements d'importance nationale ou internationale, même sans en retirer un avantage majeur au niveau de son instruction ou de son entraînement. En introduisant cette disposition d'exception, le Conseil fédéral tient compte du fait que les événements considérés ne pourraient pas avoir lieu sans l'appui de l'armée.

De surcroît, il est aussi nécessaire que le législateur intervienne dans certains autres domaines de l'instruction – celle des militaires en service long entre autres –, dans diverses dispositions sur l'engagement de l'armée en service d'appui, dans l'accomplissement des missions de l'armée en fonction des menaces dans le contexte actuel, dans les droits et les devoirs des militaires et dans le domaine des affaires sanitaires. Plusieurs dispositions de la LAAM doivent donc être modifiées. Enfin, l'appréciation lors du recrutement et lors de la remise de l'arme personnelle du potentiel de danger et d'abus que peuvent renfermer les militaires doit être améliorée.Jusqu'à présent, la Suisse ne dispose pas d'organisation comparable à l'Office fédéral de l'aviation civile pour le trafic aérien militaire. Des bases légales vont donc être créées pour une autorité du trafic aérien militaire. Celle-ci doit assurer la sécurité des Forces aériennes lors de leurs missions dans l'espace qu'elles partagent avec l'aviation civile. Elle veillera notamment à éviter tout incident ou accident dans cet espace et à garantir mieux encore la surveillance et la régulation du trafic aérien militaire. Une adaptation de la loi sur l'aviation s'impose donc.

Appui renforcé aux événements civils

Dans la foulée de la révision de la LAAM, le Conseil fédéral entend aussi renforcer l'appui apporté par l'armée aux événements civils. Cela commencera par un accroissement de la souplesse et des disponibilités de l'armée dans le sens où les recrues en phase d'instruction de base pourront, elles aussi, être engagées, et plus seulement les militaires en service long et ceux en cours de répétition. L'armée devra également pouvoir fournir des prestations dans un cadre limité lors d'événements d'importance nationale ou internationale, même sans en retirer un avantage majeur au niveau de son instruction ou de son entraînement. En introduisant cette disposition d'exception, le Conseil féwéral tient compte du fait que les événements considérés ne pourraient pas avoir lieu sans l'appui de l'armée.

De surcroît, il est aussi nécessaire que le législateur intervienne dans certains autres domaines de l'instruction – celle des militaires en service long entre autres –, dans diverses dispositions sur l'engagement de l'armée en service d'appui, dans l'accomplissement des missions de l'armée en fonction des menaces dans le contexte actuel, dans les droits et les devoirs des militaires et dans le domaine des affaires sanitaires. Plusieurs dispositions de la LAAM doivent donc être modifiées. Enfin, l'appréciation lors du recrutement et lors de la remise de l'arme personnelle du potentiel de danger et d'abus que peuvent renfermer les militaires doit être améliorée.

Source : https://www.vbs.admin.ch/content/vbs-internet/fr/die-aktuellsten-informationen-des-vbs/die-neusten-medienmitteilungen-des-vbs.detail.nsb.html/80621.html