Comparaison de l'organisation des milices de cyberdéfense de six Etats

Autor(en): **Baezner, Marie**

Objekttyp: **Article**

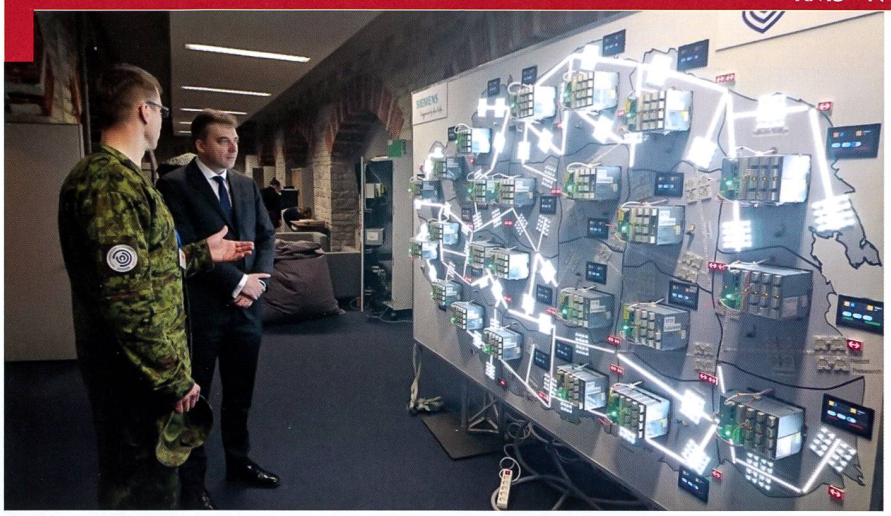
Zeitschrift: **Revue Militaire Suisse**

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

Heft 3

PDF erstellt am: **26.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-913875



Visite au centre d'instruction cyber ukrainien, où cette forme de menace est prise très au sérieux.

Cyberdéfense

Comparaison de l'organisation des milices de cyberdéfense de six Etats

Marie Baezner
Cyberdefence CYD, Base d'aide au commandement (BAC)

En août 2018, l'armée suisse lançait son Cyber Lehrgang dans le but de créer d'ici 2022 un bataillon de cyberdéfense. L'armée suisse n'est pas la seule armée à s'être lancée dans la constitution d'un élément de milice pour la cyberdéfense. En effet, l'Estonie la Finlande, la France, Israël et les Etats-Unis, entre autre, ont aussi développé une part de leur cyberdéfense à travers des éléments de milice, aussi appelés réserves.[1] Cet article[2] cherche, à travers la comparaison[3] des cinq cas susmentionnés et de la Suisse, à expliquer les avantages que constituent ces troupes de milice de cyberdéfense, ainsi que leurs défis.

Comparaison

La comparaison des milices de cyberdéfense s'est basée sur:

- L'Estonian Defence League Cyber Defence Unit[4] en Estonie;
- Les Finland Defence Forces' Cyber Conscripts en Finlande;
- la Réserve Opérationelle de Cyberdéfense et la Réserve Citoyenne de Cyberdéfense en France;
- L'Unité 8200 en Israël;
- Le Cyber Lehrgang en Suisse;
- La Cyber Mission Force au Etats-Unis.[5]

Cette comparaison s'est focalisée sur six point:

- Le processus de recrutement et d'instruction spécifique à la cyberdéfense;
- Les rôles, missions et responsabilités de ces éléments de milice;
- La taille de ces milices de cyberdéfense;
- L'organisation de leur service (temps du service et cours de répétition);
- Les liens avec le secteur privé dans le cadre du service militaire;
- Les relations post-service (si les anciens miliciens gardent contact entre eux ou avec les forces armées).

Ces six forces armées sont assez différentes des unes des autres dans leurs structures, organisations, missions et taille. Chacune a organisé ses forces de milice de cyberdéfense pour correspondre au mieux à leur propre modèle, n'empêchant toutefois pas certaines similitudes.

En ce qui concerne les processus de recrutement et l'instruction, toutes les forces armées demandent à leurs recrues d'avoir un certain niveau de prérequis dans leurs connaissances dans le domaine de la cyberdéfense avant de postuler. La différence réside dans l'étendue de ces connaissances et dans l'instruction qui suit. Cette instruction est logiquement plus longue dans les forces armées qui demandent peu de prérequis alors qu'elle est plus courte dans les forces armées qui demandent plus de prérequis. Par exemple, en France, l'instruction est de quelques semaines, alors qu'en Finlande elle est de cinq mois. Cependant, pas toutes les forces armées demandent aux candidats de passer un examen d'entrée, c'est notamment le cas pour l'Estonie, de la France et des Etats-Unis où les processus de sélection se font plus tard, durant l'instruction. De plus, pas toutes les forces

1 Dans cet article, le terme de « milice » est aussi utilisé pour désigner des unités de réserves.

2 Cet article est un extrait d'un rapport plus détaillé sur la comparaison entre les six cas d'étude. Baezner, Marie (2020): CSS Cyber Defense Report: Study on the use of reserve forces in military cybersecurity, April 2020, Center for Security Studies (CSS), ETH Zürich: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/MB_Cyber%20reserves.pdf

3 La recherche pour cet article se base uniquement sur de l'open-source. Il est aussi important de noter que certaines forces armées sont plus transparentes que d'autres sur leur milice de cyberdéfense.

4 En Estonie, l'unité de cyberdéfense étudié dans le projet de recherche fait partie d'un groupe paramilitaire, l'*Estonian Defence League*, faisant partie du système de sécurité de l'Etat estonien.

5 La Cyber Mission Force est composée de 133 équipes militaires de carrière et de milice dont des Cyber Protection Teams (21 équipes composées de US Army reserves et de Army National Guard et 5 de Air National Guard et Air Force Reserve). Il existe d'autres unités de milice de cyberdéfense dans les forces armées américaines, mais pour des raisons de temps et d'espace, seules celles de la Cyber Mission Forces ont été considérées dans cette étude.

	Estonie	Finlande	France	Israël	Suisse	Etats-Unis
Recrutement et instruction						
Armée de conscription ou de volontaires	volontaires	Conscription, les conscrits intéressés par une fonction de cyberdéfense s'annoncent pendant les premières semaines d'école de recrue	Volontaires	Conscription, sélection pour l'Unité 8200 se fait avant le service militaire par différent programmes extra-scolaires	Conscription, les conscrits intéressés par une fonction de cyberdéfense s'annoncent pendant les premières semaines d'école de recrue	Volontaires
Acquisition des connaissances de cyberdéfense avant ou pendant l'instruction	L'acquisition de connaissances se fait principalement avant de rejoindre l'unité, mais l'unité organise aussi des cours	Besoin de connaissances de base mais l'acquisition de connaissances spécifiques se fait pendant l'instruction	L'acquisition de connaissances se fait principalement avant de rejoindre la réserve avec quelques instructions complémentaires une fois accepté dans la réserve	Besoin de bonnes connaissances avant de rejoindre l'Unité 8200, puis six mois d'instructions spécifiques	Besoin de connaissances de base mais l'acquisition de connaissances spécifiques se fait pendant l'instruction	Besoin de connaissances de base mais l'acquisition de connaissances spécifiques se fait pendant l'instruction
Test d'entrée sur connaissances de cybersécurité	Non	Oui	Pas de test d'entrée mais durant l'instruction	Oui et aussi tests sur d'autres compétences	Oui et aussi tests sur d'autres compétences	Pas de test d'entrée spécifique au cyber mais durant l'instruction
Certificat de compétences	Non	Non	Non, mais équivalences de crédits universitaires	Non	Non, mais possibilité de faire un certificat à titre volontaire et aussi possibilité d'équivalences universitaires	Non
Rôles, missions et responsabilités						
Rôles	Pas de rôles définis	Cyber spécialiste	Réserviste opérationnel (coordinateur, expert, analyste ou technicien) ou réserviste citoyen	Pas de rôles définis	Spécialiste CNO, spécialiste Cyber Fusion Center, ou spécialiste Cyberdefence	Les rôles dépendent de la branche militaire et du grade
Missions	Soutien (instruction et soutien en cas d'urgence pour les institutions publiques ou privées)	Soutien (défendre les réseaux, programmation, projets, pen testing, instruction)	La réserve opérationnelle a une mission de soutien et la réserve citoyenne d'instruction et de sensibilisation	La mission dépend de l'équipe, peut être des opérations offensives et défensives, de la recherche et développement et du soutien	Soutien (développement de logiciels, forensique, recherches open source, instruction)	Conduire et soutenir des opérations offensives et défensives

armées ne fournissent à leurs cyber-soldats de certificats de compétences pouvant être reconnus dans le civil. En Estonie et en Israël, le seul fait d'appartenir à ces unités de cyberdéfense est une reconnaissance d'expertise. En France et en Suisse, les forces armées ne délivrent pas de certificats, mais les cyber-soldats peuvent faire valoir des équivalences de crédits universitaires pour ce qu'ils ont appris lors de leur instruction militaire.

Concernant les rôles, missions et responsabilités des milices de cyberdéfense, ceux-ci varient grandement d'une force armée à l'autre. Dans certaines, l'accent est mis sur les tâches que sur les rôles alors que d'autres ont des rôles clairement définis. Par exemple, en Israël ou en Estonie, les tâches des miliciens vont définir leur rôle alors qu'en France, un réserviste se verra attribuer un rôle du quel en découle certaines tâches spécifiques. Cependant, il y a une certaine similitude dans le fait que les rôles de tous les miliciens sont focalisés sur la défense ainsi que sur le soutien au personnel civil et/ou aux militaires de carrière. La principale différence est dans le fait qu'Israël et les Etats-Unis officiellement engagent leurs miliciens dans des opérations offensives. Il est toutefois nécessaire de préciser que ces deux Etats évoluent dans des contextes très différents des autres cas de cette étude.

Quant à la taille de ces milices, il est difficile d'obtenir des chiffres exacts car ceux-ci sont souvent confidentiels. Toutefois, il est possible de faire des estimations. Les Etats-Unis et Israël ont clairement les plus grandes unités, estimées respectivement à 6'300 et 5'000 soldats. Les Etats plus petits sont toutefois en train de construire leur force et leurs forces se constituent de quelques centaines de soldats.

A propos de l'organisation du service militaire et des cours de répétition, la différence majeure réside entre les forces armées de conscription et celles de volontaires. Dans les armées de conscription, les miliciens sont en général engagés pour une période plus courte que dans les armées de volontaires. L'organisation des cours de répétition dépend aussi du pays, mais parfois les milices de cyberdéfense disposent d'une organisation spéciale en comparaison avec d'autres unités. C'est notamment le cas en Finlande où les cours de répétition ont normalement lieu tous les un à cinq ans, mais les cyber-soldats ont des cours de répétition tous les deux à trois ans. Ces cycles de cours de répétition sont plus courts car la technologie évolue vite et il faut s'assurer que les cyber-soldats restent à jour dans leurs connaissances.

	Estonie	Finlande	France	Israël	Suisse	Etats-Unis
Taille de la milice de cyberdéfense						
Taille	Pas de chiffres officiels	Confidentiel	150 réservistes opérationnels (prévision d'augmenter à 400) et 150 réservistes citoyens	Estimée à 5'000 membres actifs	Environ 60 actuellement avec l'objectif de 600	Estimation de 6'300 réservistes impliqués dans la cybersécurité au sein des forces armées, mais pas de chiffres officiels
Organisation du service et cours de répétition						
Durée du service	Jusqu'à la fin du contrat ou une expulsion	255 ou 347 jours de service et 80 à 150 jours de cours de répétition jusqu'à 50 ans	Contrat de trois ans renouvelable pour les réservistes opérationnels et pas de contrat pour les réservistes citoyens	Deux ans et huit mois pour les hommes et deux ans pour les femmes, mais les membres de l'Unité 8200 restent souvent plus longtemps en signant un contrat de deux à trois ans	440 jours de service pour les sous-officiers et 680 jours pour les officiers	Contrat de huit ans
Cours de répétition	La participation aux activités n'est pas obligatoire	Cinq à six jours de cours de répétition tous les deux à trois ans avec la possibilité de participer volontairement à d'autres exercices	Cinq à 30 jours d'engagement par année pour la réserve opérationnelle, les réservistes citoyens peuvent choisir la quantité de jours d'engagement par année	Seulement ceux qui travaillent dans le civil dans la cybersécurité sont appelés pour les cours de répétition et les cas d'urgence	Trois à quatre semaines de cours de répétition par année	Les cours de répétition ont lieu un weekend par mois et une fois deux semaines par année
Liens avec le secteur privé						
Collaboration avec le secteur privé	Pas officiellement	Oui	Partenariat Réserve-Entreprise-Défense	Oui, à travers les anciens membres de l'Unité 8200	Essai d'un partenariat avec des entreprises privées pour des stages dans le cadre du Cyber Lehrgang	Partenariat privé-public pour faciliter la transition entre le service militaire et la vie civile
Collaboration avec les hautes écoles	Oui pour l'instruction	Oui pour l'instruction	Oui, dans le cadre du même partenariat que pour le secteur privé	Possible, mais pas de sources officielles	Oui pour l'instruction	Oui pour l'instruction
Après le service						
Existence d'une association d'alumni	Non, mais les membres restent en contact de manière informelle	Une association est en développement	Non	Oui, la 8200 Alumni Association (compte environ 15'000 membres)	Une association est en développement	Oui, la Military Cyber Professionals Association

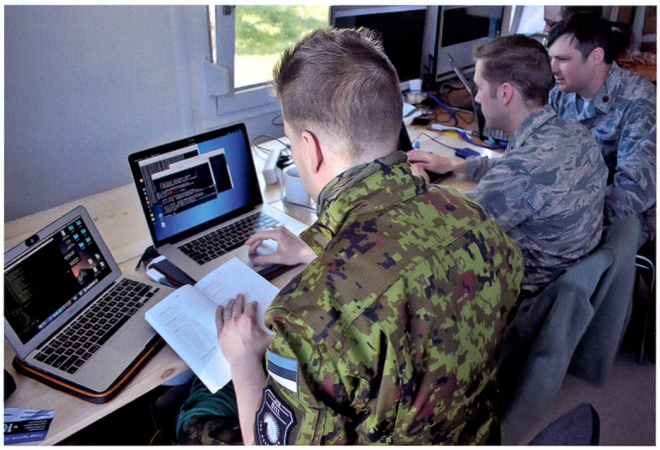
En ce qui concerne les liens entre les milices de cyberdéfense et le secteur privé, toutes les forces armées maintiennent une certaine forme de relation avec le secteur privé dans le domaine de la cybersécurité. Pour certaines forces armées, ces relations sont institutionnalisées à travers des partenariats public-privé, comme en France ou aux Etats-Unis. Pour d'autres, ces relations sont plus informelles, comme en Estonie ou en Finlande. Le cas d'Israël mérite toutefois une certaine attention pour la collaboration étroite entre les forces armées et les firmes et startups de cybersécurité fondées par des alumni de l'Unité 8200. Les partenariats public-privé ont surtout pour but de favoriser la coopération entre le secteur privé et les forces armées, mais aussi de faciliter la transition des miliciens entre la vie militaire et la vie civile et vice-versa. Ces partenariats sont aussi souvent étendus aux hautes écoles avec des échanges d'enseignants ou de programmes d'enseignement.

Concernant l'après-service militaire, les opportunités pour les miliciens de rester en contact varient. Aux Etats-Unis et en Israël, il existe des associations d'alumni qui organisent régulièrement des événements de réseautage. En Finlande et en Suisse, de telles associations sont en cours de développement alors qu'en France et en Estonie, elles n'existent tout simplement pas.

Avantages

Alors que les milices de cyberdéfense ont plusieurs formes et organisations, elles présentent toutes certains avantages pour les états qui décident de les mettre en place. Le premier avantage est économique. En effet, avoir une force de cyberdéfense sous la forme d'une milice permet aux forces armées d'économiser sur les coûts de

Un centre d'excellence cyber a été mis sur pied par l'OTAN à Tallinn, en Estonie.



personnels et d'instruction. De manière générale, une force de milice de cyberdéfense coûterait moins cher qu'une force uniquement de militaires de carrière ou de sous-traitants. Les miliciens viennent avec leurs connaissances de cybersécurité, ce qui réduit les temps d'instruction et reçoivent des salaires plus bas que les professionnels. Un système de milice dans la cyberdéfense permet aussi de constituer relativement rapidement un groupe d'experts pour un prix raisonnable.

Le deuxième avantage est qu'une milice de cyberdéfense permet aux forces armées de combler le manque de main-d'œuvre dans ce secteur. En effet, (ISC)² a estimé, dans une étude de 2018, qu'il manquait environ trois millions de main-d'œuvre dans le domaine de la cybersécurité à travers le monde.[6] Ce manque de main-d'œuvre met le secteur public, forces armées inclues, en compétition directe avec le secteur privé pour engager les meilleurs experts. Dans cette compétition, les forces armées sont particulièrement désavantagées car elles ont des ressources plus limitées et des conditions de travail qui ne sont pas toujours attractives. Dans ce contexte, une force de cyberdéfense sous la forme d'une milice est un avantage car il permet aux forces armées d'avoir accès à des experts pour une durée limitée et permet aussi d'attirer des experts qui auraient été intéressés par un poste de militaire mais qui étaient rebutés pour quelques raisons.

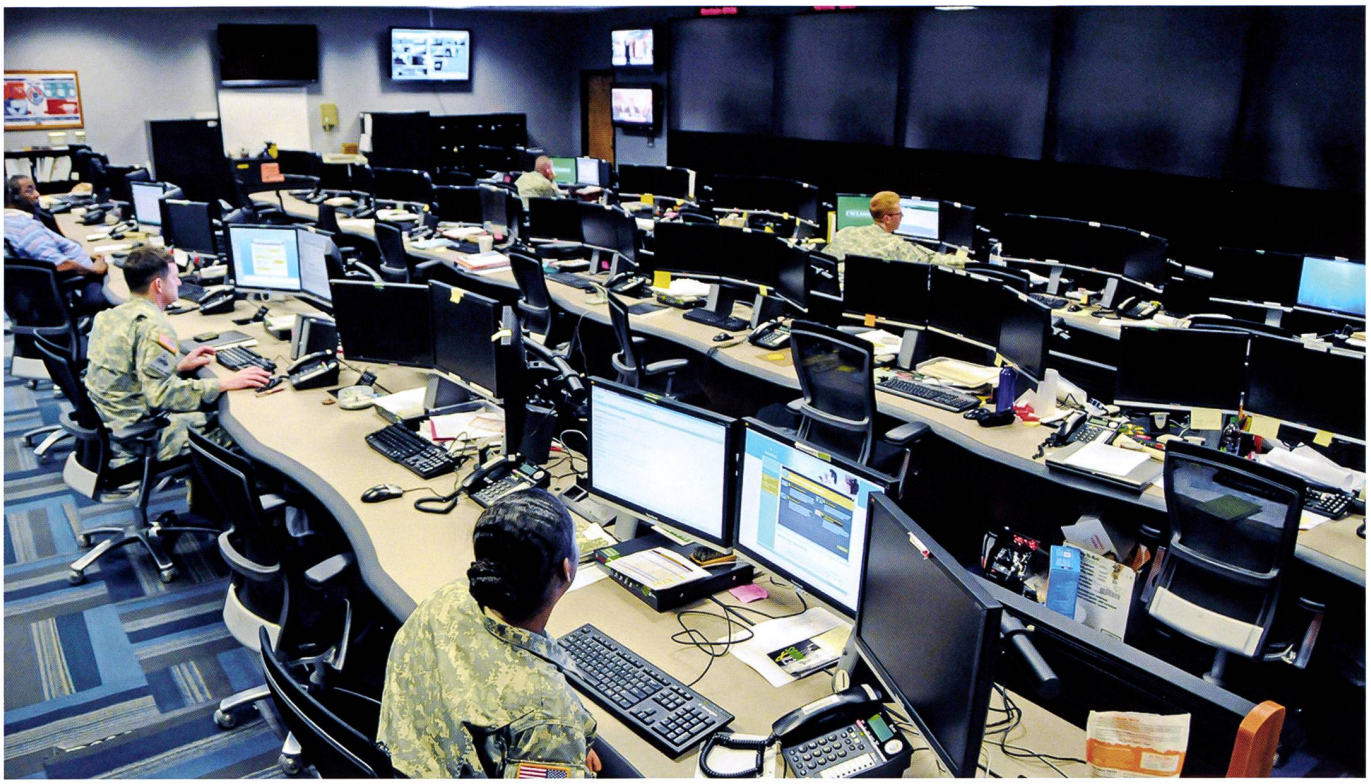
Pour finir, le troisième avantage est le fait qu'un système de milice rapproche les forces armées de la société civile. Effectivement, le milicien se situe entre le monde militaire et le monde civil.[7] Ces deux mondes peuvent donc profiter des connaissances apprises des deux côtés. Les miliciens peuvent faire profiter leur employeur des connaissances acquises au service militaire et vice versa. Avoir un système de milice encourage aussi la collaboration entre les forces armées et le secteur privé en apportant une meilleure compréhension de chaque monde des deux côtés. Une milice de cyberdéfense sert aussi de plateforme de réseautage. Les experts faisant leur service militaire ensemble apprennent à se connaître et peuvent maintenir ces liens quand ils retournent à la vie civile. Ces liens sociaux sont utiles aux miliciens dans leur vie professionnelle (ex: recherche d'emploi) mais aussi au secteur de la cybersécurité. En effet, les miliciens peuvent devenir des points de contact informels entre les entreprises et permettre un possible échange d'informations informel en cas de crise.

Défis

Bien que les milices de cyberdéfense présentent des avantages pour les forces armées, elles représentent aussi des défis. La comparaison des milices des six états a mis en évidence sept défis communs. Le premier défi concerne le recrutement et la gestion des miliciens. Ce n'est pas tout d'avoir une milice de cyberdéfense, encore faut-il recruter les bonnes personnes, les convaincre et les retenir. De plus, les forces armées ont peut-être déjà des experts en cybersécurité dans leurs rangs, sans le savoir, le défi est de se donner les moyens de les identifier et de leur donner la possibilité de changer de fonction s'ils le désirent.

6 (ISC)², 2018. Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens, (ISC)² Cybersecurity Workforce Study. (ISC)².

7 Lomsky-Feder, E., Gazit, N., Ben-Ari, E., 2008. Reserve Soldiers as Transmigrants: Moving between the Civilian and Military Worlds. Armed Forces Soc. 34, 593–614. https://doi.org/10.1177/0095327X07312090



Le second défi se rapporte à l'intégration de cette milice de cyberdéfense dans les structures militaires existantes et la coordination entre la milice et ces structures. Pour beaucoup d'états, la cyberdéfense est un nouvel élément qui doit être intégré dans les structures militaires. Le défi est donc de trouver une variante qui fonctionne tout en sachant que la cyberdéfense est un domaine transversal qui ne peut être considéré comme un élément isolé.

Le troisième défi relate des compétences et de l'instruction de la milice de cyberdéfense. Dans l'établissement d'une telle milice, les forces armées recrutent une main-d'œuvre hétérogène aillant déjà un certain niveau de connaissances du domaine. Le défi consiste donc à assurer que les miliciens acquièrent une certaine base commune de connaissance pour leurs missions. Cette instruction peut se faire entièrement au sein de l'armée tout comme elle peut se faire en collaboration avec le secteur privé et/ou les hautes écoles.

Le quatrième défi concerne les risques de sécurité que représente l'emploi de miliciens dans la cyberdéfense. En effet, les miliciens vont avoir accès, dans le cadre de leur service militaire, à des informations classifiées et les forces armées disposent moins de contrôle sur eux que sur les employés permanents. Le défi est donc la gestion du risque que pourraient représenter ces miliciens. Dans les six cas étudiés, tous font passer un contrôle de sécurité aux miliciens. Cependant, certains prennent des mesures supplémentaires pour réduire ces risques, comme de s'assurer que les miliciens sont toujours accompagnés d'un employé permanent (militaire ou civil).

Le cinquième défi touche à l'équilibre entre coûts et bénéfices d'une milice de cyberdéfense. En effet, une milice coûte en principe moins cher qu'une armée de professionnels, mais il est nécessaire d'optimiser le temps que passent les miliciens au service militaire. Ce temps est relativement limité et donc les forces armées doivent s'assurer que ce temps soit utilisé le mieux possible. Cela peut être maximiser en focalisant les instructions de cyberdéfense sur ce qui est uniquement nécessaire pour la mission des miliciens. De plus, si l'instruction se focalise sur la pratique, celle-ci permet aux miliciens d'apprendre tout en étant déjà en poste.

Le sixième défi concerne la disponibilité des miliciens. C'est un défi qui touche aussi à la gestion des miliciens pour les cours de répétition. Pour assurer leur disponibilité, il est dans l'intérêt des forces armées de collaborer avec les employeurs du secteur privé pour leur faire comprendre la plus-value d'avoir un ou des miliciens parmi leurs employés et de les laisser aller aux cours de répétition.

Le dernier défi adresse la fidélisation des miliciens de cyberdéfense. Dans le secteur de la cybersécurité, où les experts peuvent obtenir des salaires plus importants dans le privé, il est nécessaire pour les forces armées de retenir leurs miliciens et de les motiver à revenir à chaque cours de répétition. Ce défi consiste principalement à trouver des éléments de motivation, comme une médaille ou distinction cyber, ou des missions motivantes, pour fidéliser les miliciens. Cette fidélisation peut aussi se prolonger au-delà du service militaire à travers une association d'alumni qui développe un sentiment d'appartenance à un groupe spécial.

Ces défis ne concernent pas toujours que les milices de cyberdéfense, mais parfois aussi d'autres fonctions de milice. Ces défis restent néanmoins des points que les forces armées doivent garder en tête dans l'établissement d'une telle milice.

Ci-dessus : Exercices cyber des armées française (haut) et italienne (bas).

La photo ci-dessous présente un état-major américain.

Conclusion

Etablir une milice de cyberdéfense présente certes certains avantages (coûts moindre, réduction dans le manque de main-d'œuvre et augmentation de la collaboration avec le secteur privé), mais aussi contient des défis non-négligeables. L'étude des milices de cyberdéfense en Estonie, Finlande, France, Israël, Suisse et Etats-Unis a permis de montrer que l'organisation, la structure et le développement de ces milices dépendaient beaucoup du contexte. En effet, même si certains états se sont inspirés des pratiques d'autres états, tous ont développé leur propre forme de milice de cyberdéfense démontrant qu'il n'y a pas un modèle unique à appliquer. De plus, ces milices se présentent comme des solutions pour réduire le manque de main-d'œuvre dans le domaine de la cybersécurité. Ces milices permettent aux forces armées de constituer une réserve d'experts qui peuvent apporter leurs expériences du civil et entretenir leurs connaissances durant leur service militaire. Finalement, cette étude a révélé que l'établissement de milices de cyberdéfense était un travail en cours. Le développement de ces milices est une évolution récente pour les forces armées. Ces dernières sont encore à se chercher et à les ajuster pour mieux correspondre à leurs buts stratégiques et à leurs ressources.

M. B.