digitalswitzerland

Département fédéral de la défense,
Protection de la population et sports DDPS
3003 Berne

Envoi par mail à:
Hans.wipfli@vtg.admin.ch

Zurich, le 8 mars 2024

Consultation sur la modification de la loi sur l'armée et l'administration militaire

Réaction concernant l'art. 95 de la loi sur l'armée et l'administration militaire (AP-LAAM)

Madame la Présidente de la Confédération Amherd,
Monsieur Wipfli,
Mesdames et Messieurs

Nous nous référons à la consultation que vous avez ouverte sur **la modification de la loi sur l'armée et l'administration militaire, l'ordonnance de l'Assemblée fédérale concernant l'administration de l'armée et l'organisation de l'armée** du 22 novembre 2023. digitalswitzerland saisit volontiers l'occasion de prendre position sur l'avant-projet de loi (AP-LAAM). Nous nous référons à l'art. 95 AP-LAAM, qui doit créer la base permettant de saisir des ressources de tiers ou d'en restreindre l'utilisation, même en temps de paix, afin de garantir la continuité de l'exploitation et la résilience de l'armée et de l'administration militaire face à des menaces diverses (en particulier face à des cyber-incidents et -attaques).

digitalswitzerland salue la révision proposée de la loi sur l'armée et l'administration militaire. Nous comprenons que la guerre hybride exige de nouvelles mesures de politique de sécurité. **Toutefois, du point de vue de digitalswitzerland, l'art. 95 AP-LAAM doit être révisé**. D'une part, les scénarios relatifs aux situations de cybermenace doivent être connus par tous, afin d'augmenter la compréhension et la confiance des mesures de réquisition et de restriction dans l'économie et la population. D'autre part, le projet prévoit des possibilités d'intervention relativement importantes, sans que les organisations concernées puissent en contrepartie être suffisamment consultées ou faire opposition.

Guerre hybride : les cybermenaces et leur qualification

L'un des effets les plus déstabilisants de la guerre hybride est que le fait de savoir clairement si l'on se trouve en temps de paix ou de conflit ne débouche pas sur une réponse de type binaire, mais que l'on se trouve dans une ambiguïté et une incertitude permanentes. La prochaine attaque est aujourd'hui à un clic de souris, tandis que les chars sont visibles par tous à la frontière. Cet état de fait est renforcé par le fait que l'appartenance des agresseurs à un État ou à une organisation privée n'est parfois pas claire, et que les cyberattaques sont souvent liées à des coûts modestes - et très faibles par rapport aux opérations conventionnelles. Bien que le potentiel de dommages des moyens cybernétiques en cas de guerre soit tendanciellement surestimé[1], l'ambiguïté qui en résulte érode le sentiment de sécurité.

[1] Siehe Maschmeyer, L. (2023): Hybrider Krieg - Vorstellung und Wirklichkeit. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse332-DE.pdf

Partant du principe qu'il existe une situation de cybermenace constante et latente dans la conduite de la guerre hybride, la question se pose de savoir quel niveau d'escalation doit se produire pour qu'une réquisition ou une restriction par le Conseil fédéral apparaisse comme proportionnée en temps de paix.

- Par exemple, une attaque DDOS persistante sur le site web portal-armee.ch remplit-elle les critères d'un tel niveau d'escalation? Les militaires ne pourraient plus avoir accès aux informations concernant les cours de répétition et les ordres de marche. Le transport et la répartition des forces sont ainsi menacés.
- L'attaque doit-elle déjà être en cours ou avoir eu lieu?
- Faut-il prendre des mesures préventives, par exemple sur la base d'informations collectées par les services de renseignement?

Il s'agit en substance de définir **une situation extraordinaire en temps de paix en ce qui concerne les cybermenaces**, qui légitimerait des interventions massives dans des organisations privées. Nous connaissons une catégorisation issue de la pandémie[2], mais pas (encore) de scénarios de menace de cyberattaques.

C'est pourquoi nous recommandons que la Confédération publie une catégorisation exemplaire et fiable des cybermenaces. Digitalswitzerland considère une telle catégorisation comme une mesure de confiance qui permet de mieux faire connaître les menaces de cyberattaques dans l'économie et la société et de sensibiliser ainsi la population.

Exigence de proportionnalité:

Les mesures demandées par l'armée peuvent constituer une intervention massive dans la liberté économique des personnes et des entreprises concernées. Cela pose problème, car les interventions dans la liberté économique ne sont autorisées qu'à des conditions strictes, notamment lorsqu'elles sont prises en temps de paix (cf. art. 36 Cst.). Afin de garantir la proportionnalité des mesures, digitalswitzerland demande que le Conseil fédéral consulte les organisations concernées avant de décider d'autoriser des mesures en vertu de l'art. 95 AP-LM en temps de paix. C'est la seule manière pour le Conseil fédéral de bien saisir et de pondérer les intérêts des personnes concernées. Cela est indispensable pour l'examen de la proportionnalité ou de l'acceptabilité des mesures. Nous partons certes du principe que la loi fédérale sur la procédure administrative (LPA) contient implicitement ces droits (notamment le droit de consulter le dossier et d'être entendu). Comme l'atteinte à la liberté économique est massive, nous sommes d'avis que la notion d'"indemnité équitable" porte en elle une ambiguïté qui ne représente pas correctement l'interdépendance de l'armée et de l'économie en temps de paix et ne va pas dans le sens de l'idée de milice, respectivement qui n'apprécie pas suffisamment cette collaboration profitable.

C'est pourquoi nous recommandons de mentionner explicitement le droit d'être entendu et de remplacer le terme "indemnisation équitable" par "indemnisation couvrant les coûts", ce qui constitue une mesure importante pour instaurer la confiance avec les organisations concernées.

En résumé, nous proposons de modifier l'art. 95 AP-LAAM comme suit :
Art. 95 AP-LAAM, al. 2; *L'administration militaire et l'armée ne peuvent faire usage des compétences visées à l'al. 1 que dans la mesure où cela est absolument nécessaire et qu'elles ne peuvent pas assurer le maintien de la continuité de l'exploitation et de la résilience de l'armée contre les cybermenaces par leurs propres moyens ou par des réglementations contractuelles avec des tiers. L'ordonnance de mesures selon l'al. 1* requiert l'approbation du Conseil fédéral *dans le cadre de la procédure d'ordonnance concrète. Le Conseil fédéral*

[2] La fiche d'information de l'Office fédéral de la santé publique décrit, sur la base de la loi sur les épidémies, les conditions de survenance de la situation normale, particulière et extraordinaire et les compétences qui en découlent pour le Conseil fédéral. URL: https://www.newsd.admin.ch/newsd/message/attachments/60477.pdf

soumet préalablement les mesures proposées en temps de paix aux personnes concernées pour avis et tient compte de cet avis dans la décision d'autorisation.

Art. 95 AP-LAAM, al. 3 : *La Confédération verse des indemnités couvrant les coûts de la limitation ou de l'interdiction d'utilisation ainsi que de la réquisition des biens réquisitionnés.*

Art. 95 AP-LAAM, al. 6 (nouveau) : *La Confédération établit et publie une catégorisation des scénarios de cybermenace qui justifient une mesure de réquisition ou de restriction en temps de paix.*

Nous vous prions de tenir compte de la problématique exposée lors de l'amélioration du projet sur la base de la procédure de consultation. digitalswitzerland renvoie volontiers à la lettre d'economiesuisse, de l'ISSS et de Switch.

Nous vous remercions de l'attention que vous porterez à nos demandes et vous prions de croire, Madame, Monsieur, en l'expression de notre considération distinguée.

Stefan Metzger
Managing Director digitalswitzerland
stefan@digitalswitzerland.com

Guillaume Gabus
Public Affairs & Extended Management
guillaume@digitalswitzerland.com

À propos de digitalswitzerland

digitalswitzerland est une initiative intersectorielle à l'échelle nationale qui vise à transformer la Suisse en une nation numérique de premier plan. Avec notre réseau de 170+ membres d'association et partenaires non politiques, dont plus de 1 000 cadres supérieurs, nous sommes engagés dans plus de 25 projets pour inspirer, initier, co-créer et conduire le changement numérique en Suisse