digitalswitzerland

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
3003 Bern

Einreichung per Mail an:
Hans.wipfli@vtg.admin.ch

Zürich, 8. März 2024

Vernehmlassung zur Änderung des Militärgesetzes

Rückmeldung bezüglich Art. 95 Militärgesetz (VE-MG)

Sehr geehrte Frau Bundespräsidentin Amherd,
Sehr geehrter Herr Wipfli,
Sehr geehrte Damen und Herren,

Wir beziehen uns auf die von Ihnen eröffnete Vernehmlassung **Änderung des Militärgesetzes, der Verordnung der Bundesversammlung über die Verwaltung der Armee und der Armeeorganisation** vom 22. November 2023. Gerne nimmt digitalswitzerland hiermit die Gelegenheit wahr, zur Änderung im Gesetzesentwurf (VE-MG) Stellung zu nehmen. Wir beziehen uns dabei auf Art. 95 VE-MG, welche die Grundlage schaffen soll, um auch in Friedenszeiten Ressourcen von Dritten zu beschlagnahmen oder deren Nutzung einzuschränken zur Gewährleitung der Betriebskontinuität und Resilienz der Armee, der Militärverwaltung aufgrund verschiedenartigen Bedrohungen (insbesondere gegenüber Cybervorfällen und -angriffen).

digitalswitzerland begrüsst die vorgeschlagene Revision des Militärgesetzes. Wir können nachvollziehen, dass die hybride Kriegsführung neue sicherheitspolitischen Massnahmen verlangt. ***Aus Sicht von digitalswitzerland muss jedoch Art. 95 VE-MG überarbeitet werden.*** Einerseits müssen Szenarien zu Cyberbedrohungslagen allgemein bekannt sein, um das Verständnis und das Vertrauen von Requisitions- und Einschränkungsmassnahmen in der Wirtschaft und Bevölkerung zu steigern. Andererseits sieht die Vorlage relativ weitgehende Eingriffsmöglichkeiten vor, ohne dass betroffene Firmen im Gegenzug ausreichend angehört werden oder Einsprachen erheben können.

Hybride Kriegsführung: Cyberbedrohungen und deren Qualifizierung

Eine der destabilisierendsten Wirkungen der hybriden Kriegführung ist, dass die klare Feststellung, ob man sich in Friedenszeiten oder in einem Konflikt befindet, keine binäre Antwort mit sich zieht, sondern dass man sich in einer ständigen Ambiguität und Unsicherheit befindet. Der nächste Angriff ist heute einen Mausklick entfernt, währenddessen Panzer an der Grenze für alle sichtbar sind. Verstärkt wird dieser Umstand dadurch, dass die Zugehörigkeit der Angreifer zu einem Staat oder einer privaten Organisation teilweise nicht eindeutig ist, und Cyberangriffe oftmals mit niedrigen - und im Vergleich zu konventionellen Operationen sehr niedrigen Kosten - verbunden sind. Obschon das Schadenspotenzial von Cybermitteln im Kriegsfall tendenziell überschätzt wird[1], zersetzt die resultierende Ambiguität das Sicherheitsgefühl.

[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

Ausgehend davon, dass in der hybriden Kriegsführung eine stetige, latente Cyber-Bedrohungslage existiert, stellt sich die Frage, was für eine Eskalationsstufe eintreten muss, damit eine Requisition oder Einschränkung durch den Bundesrat in Friedenszeiten als verhältnismässig erscheint.

- Erfüllt z.B. eine anhaltende DDOS-Attacke auf die Webseite portal-armee.ch die Kriterien einer solchen Eskalationsstufe? Angehörige der Armee könnten nicht mehr auf Informationen bezüglich WKs und Marschbefehle zugreifen. Dadurch sind Transport und Verteilung der Kräfte gefährdet.
- Muss der Angriff schon im Gang sein, bzw. bereits geschehen sein?
- Sollen, z.B. aufgrund von nachrichtendienstlich gesammelten Informationen, vorbeugend Massnahmen getroffen werden?

Im Kern geht es um die Definition einer **ausserordentlichen Lage in Friedenszeiten in Bezug auf Cyberbedrohungen,** die massive Eingriffe in private Unternehmen legitimiert. Wir kennen eine Kategorisierung aus der Pandemie[2], aber (noch) nicht aus Bedrohungsszenarien von Cyberangriffen.

Deswegen empfehlen wir, dass der Bund eine beispielhafte und belastbare Kategorisierung von Cyberbedrohungen veröffentlicht. Digitalswitzerland versteht eine solche Kategorisierung als eine vertrauenssteigernde Massnahme, welche die Bedrohungen durch Cyberangriffe in der Wirtschaft und Gesellschaft besser bekannt macht und dadurch die Bevölkerung sensibilisiert.

Erfordernis der Verhältnismässigkeit:

Die von der Armee beantragten Massnahmen können einen massiven Eingriff in die Wirtschaftsfreiheit der betroffenen Personen und Unternehmen darstellen. Dies ist problematisch, da Eingriffe in die Wirtschaftsfreiheit nur unter strengen Voraussetzungen zulässig sind, insbesondere wenn sie in Friedenszeiten ergriffen werden (vgl. Art. 36 BV). Um die Verhältnismässigkeit der Massnahmen zu gewährleisten, fordert digitalswitzerland, dass der Bundesrat die betroffenen Organisationen vor einer Entscheidung über die Bewilligung von Massnahmen nach Art. 95 VE-MG in Friedenszeiten anhört. Nur so kann der Bundesrat die Interessen der Betroffenen richtig erfassen und gewichten. Dies ist unerlässlich für die Prüfung der Verhältnismässigkeit bzw. Zumutbarkeit der Massnahmen. Zwar gehen wir davon aus, dass das Bundesverwaltungsverfahrensgesetz (VwVG) diese Rechte implizit beinhaltet (insbesondere Recht auf Akteneinsicht und Anhörung).
Weil der Eingriff in die Wirtschaftsfreiheit massiv ist, sind wir der Meinung, dass der Begriff “angemessene Entschädigung” eine Ambiguität mit sich trägt, welche die gegenseitige Abhängigkeit von Armee und Wirtschaft in Friedenszeiten und im Sinne des Milizgedankens nicht richtig darstellt, beziehungsweise die gewinnbringende Kollaboration nicht genügend würdigt.

Deswegen empfehlen wir, die explizite Erwähnung eines Anhörungsrechts, sowie das Ersetzen des Begriffs “angemessen Entschädigung” durch “kostendeckende Entschädigung” als wichtige vertrauensbildende Massnahme gegenüber den betroffenen Organisationen.

Zusammenfassend schlagen wir vor Art. 95 VE-MG folgendermassen zu ändern:
Art. 95 VE-MG Abs. 2; *Die Militärverwaltung und die Armee dürfen von den Kompetenzen gemäss Absatz 1 nur soweit Gebrauch machen, als dies unbedingt erforderlich ist und sie die Erhaltung der Betriebskontinutität und Resilienz der Armee gegen Cyberbedrohungen weder mit eigenen Mitteln erfüllen noch im Rahmen vertraglicher Regelungen mit Dritten beschaffen können. ~~Solche~~ Die Anordnung von Massnahmen gemäss Abs. 1 bedarf ~~bedürfen~~ im Vorgang zur konkreten Anordnung der Genehmigung durch den Bundesrat. Der*

[2] Das Faktenblatt des Bundesamtes für Gesundheit beschreibt, gestützt auf das Epidemiengesetz, die Voraussetzungen für den Eintritt der normalen, besonderen und ausserordentlichen Lage und die daraus für den Bundesrat abgeleiteten Kompetenzen. URL: https://www.newsd.admin.ch/newsd/message/attachments/60477.pdf

Bundesrat unterbreitet die beantragten Massnahmen in Friedenszeiten den betroffenen Personen vorgängig zur Stellungnahme und berücksichtigt die Stellungnahme im Bewilligungsentscheid.

Art. 95 VE-MG Abs. 3: *Der Bund leistet für die Einschränkung oder das Verbot der Nutzung sowie die Requisition des Requisitionsgutes ~~angemessene~~ kostendeckende Entschädigung.*

Art. 95 VE-MG Abs. 6 (neu): *Der Bund erstellt und veröffentlicht eine Kategorisierung von Cyberbedrohungsszenarien, die eine Requisition- oder Einschränkungsmassnahme in Friedenszeiten begründen.*

Wir bitten Sie bei einer Nachbesserung der Vorlage aufgrund der Vernehmlassung die dargelegte Problematik zu berücksichtigen. Gerne verweist digitalswitzerland auf das Schreiben von economiesuisse und der Switch AG.

Für Ihre Kenntnisnahme und für die wohlwollende Prüfung und Berücksichtigung unserer Anliegen, sehr geehrten Damen und Herren, danken wir Ihnen.

Stefan Metzger
Managing Director digitalswitzerland
stefan@digitalswitzerland.com

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

Über digitalswitzerland

digitalswitzerland ist eine schweizweite, branchenübergreifende Initiative, welche die Schweiz als weltweit führenden digitalen Innovationsstandort stärken und verankern will. Unter dem Dach von digitalswitzerland arbeiten an diesem Ziel mehr als 170 Organisationen, bestehend aus Vereinsmitgliedern und politisch neutralen Stiftungspartnern, transversal zusammen. digitalswitzerland ist Ansprechpartner in allen Digitalisierungsfragen und engagiert sich für die Lösung vielfältiger Herausforderungen.