

E-Mail an Mitglieder des Deutschen Bundestages am 7. Januar 2026

Sehr geehrte:r...,

Die Open Source Business Alliance (OSBA) – Bundesverband für digitale Souveränität e.V. ist der Verband der deutschen Open-Source-Industrie und vertritt über 260 Mitgliedsunternehmen, die jährlich mehr als 126 Milliarden Euro erwirtschaften. Gemeinsam mit Partnerorganisationen setzen wir uns dafür ein, die zentrale Bedeutung von Open Source Software und offenen Standards für einen erfolgreichen digitalen Wandel im öffentlichen Bewusstsein nachhaltig zu verankern. Denn Open Source und offene Standards sind zwingende Grundlagen für digitale Souveränität, Innovationsfähigkeit und Sicherheit im digitalen Wandel und damit die Antwort auf eine der größten Herausforderungen unserer Zeit.

Ich schreibe Ihnen heute, weil kommende Woche der "Gesetzentwurf zur beschleunigten Planung und Beschaffung für die Bundeswehr" in 2./3. Lesung beschlossen werden soll.

**Wir möchten Ihnen gerne auf diesem Weg unsere Einschätzung zum "Gesetzentwurf zur beschleunigten Planung und Beschaffung für die Bundeswehr" mitteilen**, siehe unten. Wir haben diese Einschätzung auch mit dem Büro von XXX geteilt, mit dem wir in regelmäßigem Austausch stehen.

Der Gesetzentwurf ist gemeinsam mit dem "Gesetzentwurf zur Beschleunigung der Vergabe öffentlicher Aufträge" Teil eines Pakets zur Vergabebeschleunigung:

<https://www.bundestag.de/dokumente/textarchiv/2025/kw41-de-vergaben-beschleunigen-1111830>

Hier finden Sie die Stellungnahme unseres Verbandes zum "Gesetzentwurf zur Beschleunigung der Vergabe öffentlicher Aufträge":

<https://osb-alliance.de/publikationen/statements/stellungnahme-zum-entwurf-des-gesetzes-zur-beschleunigung-der-vergabe-oeffentlicher-auftraege>

\*\*\*\*\*

**„Streitkräfte sind für die meisten ihrer Aktivitäten auf Software angewiesen**, von administrativen Aufgaben und Logistik bis hin zur Kriegsführung: So sind etwa Lagebildplattformen unverzichtbar geworden und kaum ein Panzer, Kriegsschiff oder Kampfflugzeug funktioniert ohne Software. Diese Softwareprodukte sind das Ergebnis komplexer Lieferketten aus Lieferanten, Dienstleistern und Softwarekomponenten, die sich der Kontrolle der Streitkräfte entziehen. Folglich hängt die Sicherheit eines Militärs auch von der Sicherheit der zahlreichen Software-Anbieter, Dienstleister sowie Entwickler:innen und Maintainer:innen von Softwarekomponenten ab.“ [1]

Ein Großteil der Software, die in Kampfmitteln und Geräten verbaut ist und in der Bundeswehr-Verwaltung genutzt wird, ist **Closed Source Software aus**

**den USA.** Das bedeutet auch, dass zentrale Systeme auf Druck aus den USA manipuliert, blockiert oder abgeschaltet werden könnten. Die F35-Flugzeuge beispielsweise müssen mit einem Cloud-System verbunden sein, um einsatzfähig zu sein. [2]

Es gibt bereits verschiedene **Präzedenzfälle, in denen Kampfsysteme anderer Staaten durch die USA lahmgelegt wurden**, indem Software blockiert wurde:

- „Software-Defined Kill-Switch“: Die F16-Kampfflugzeuge der Ukraine sind auf Softwaresupport angewiesen, diesen hatten die USA zwischenzeitlich gesperrt [3]
- USA hatten zwischendurch auch Zugriff der Ukraine auf Satellitenbildgebungs-Software gesperrt [4]

**Closed Source Software kann nicht unabhängig betrieben, weiter entwickelt, angepasst, gewartet und überprüft werden.** Das birgt etliche Risiken, u.a. für die Manipulation der genutzten Software [5].

Nach den jüngsten Beispielen vom Internationalen Strafgerichtshof oder auch deutschen NGOs wie HateAid, die von US-Präsident Trump mit Sanktionen belegt und in diesem Zusammenhang zum Teil auch von zentralen Softwareplattformen ausgesperrt wurden, muss die reale Gefahr berücksichtigt werden, **dass die USA im Konfliktfall die Einsatzfähigkeit deutscher Streitkräfte durch ein Abschalten oder eine Manipulation von Software beeinträchtigen könnten.**

Vor diesem Hintergrund ist **der Einsatz von Open Source Software ein sicherheitspolitisches Muss:** Bei Open Source Software kann der Quellcode jederzeit eingesehen, angepasst, verändert, weiter gegeben und auch unabhängig überprüft werden.

Wenn die Bundeswehr die Beschaffung beschleunigt, aber weiterhin hauptsächlich Produkte beschafft, in denen US-amerikanische Closed Source Software verbaut ist, **gefährdet sie nicht nur die digitale Souveränität, sondern auch die außenpolitische Sicherheit und die Verteidigungsfähigkeit.**

Dabei hat die Bundesregierung sich im **Koalitionsvertrag** das Ziel gesetzt, die digitale Souveränität zu stärken. Im Koalitionsvertrag hat die Bundesregierung festgelegt, dass sie Open Source Software gezielt vorantreiben und „ambitionierte Ziele für Open Source“ festlegen will.

Der "Geszentwurf zur beschleunigten Planung und Beschaffung für die Bundeswehr" sieht in §11 Abs. 2 u.a. eine Klausel vor, nach der **Auftraggeber einen wertmäßigen Anteil des Waren- beziehungsweise Dienstleistungsursprungs in der EU festlegen können.** Die Motivation hinter dieser Regelung ist sicher nachvollziehbar, sie trägt aber kaum zur technologischen Souveränität bei, wenn die in den Produkten verbaute oder

genutzte Software von Closed-Source-Anbietern aus den USA stammt und somit nicht unabhängig genutzt oder überprüft werden kann.

[1]

[https://www.swp-berlin.org/publications/products/studien/2025S14\\_Achillesfers\\_eSoftware-Lieferkette.pdf](https://www.swp-berlin.org/publications/products/studien/2025S14_Achillesfers_eSoftware-Lieferkette.pdf)

[2] <https://www.derstandard.de/story/3000000261201/nein-die-f-35-braucht-gar-keinen-kill-switch>

[3] <https://medium.com/@Forensic-Archive/us-temporarily-cut-ukraines-intelligence-access-f-16s-stopped-working-himars-went-dark-b4849d2b74d7>

[4] <https://www.reuters.com/world/us-aerospace-firm-maxar-disables-satellite-photos-ukraine-2025-03-07/>

[5] <https://www.propublica.org/article/microsoft-digital-escorts-pentagon-defense-department-china-hackers>