

Kleine Anfrage

der Abgeordneten Kurt Kleinschmidt, Dr. Daniel Zerbin, Jörg Zirwes, Gerold Otten, Heinrich Koch, Sven Wendorf, Rüdiger Lucassen, Jan Ralf Nolte, Mirco Hanker und der Fraktion der AfD

Aktueller Stand Schutz von sicherheits- und verteidigungsindustriellen Schlüsseltechnologien

Die Bundesregierung hat in ihrem „Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie“ (Bundestagsdrucksache 19/17296) die Notwendigkeit betont, die Abhängigkeit von ausländischen Informationstechnologien zu reduzieren und die digitale Souveränität sowie die Resilienz gegenüber hybriden Bedrohungen zu stärken. Hervorgehoben wird, dass bestehende Mechanismen der Außenwirtschaftsverordnung (AWV) lediglich reaktiv wirken und daher keine hinreichende Vorsorge gegen drohende Ausverkäufe sicherheits- und verteidigungsindustrieller Schlüsseltechnologien leisten können. Die Bundesregierung kündigt deshalb an, strategisch einsetzbare Instrumente zu entwickeln, die bereits in frühen Stadien von Schlüsseltechnologien ansetzen. Ein wesentlicher Bestandteil dieser Überlegungen ist die Einrichtung eines IT-Sicherheitsfonds, um unerwünschten Übernahmen frühzeitig begegnen zu können.

Vor diesem Hintergrund stellt sich den Fragestellern die Frage, welche Kriterien und Verfahren die Bundesregierung für die Identifizierung relevanter Technologien vorsieht, welche rechtlichen und europäischen Rahmenbedingungen beachtet werden, wie die institutionelle und finanzielle Ausgestaltung des geplanten IT-Sicherheitsfonds konzipiert ist und welche konkreten Fortschritte bislang erreicht wurden. Darüber hinaus ist von Interesse, welche quantitativen Zielgrößen definiert sind und wie die Reduktion der Abhängigkeit von ausländischen Informationstechnologien gemessen wird.

Wir fragen die Bundesregierung:

1. Nach welchen Kriterien identifiziert die Bundesregierung Technologien, die „heute bereits erkennbar, aber erst zukünftig in der Masse relevant und produktiv eingesetzt werden“ (vgl. Bundestagsdrucksache 19/17296, S. 7)?
2. In welchem Stadium befindet sich die geplante Einrichtung eines IT-Sicherheitsfonds (rechtliche Vorprüfung, Finanzierungsmodell, institutionelle Zuständigkeit)?
3. Wie ist der aktuelle Stand der praktischen Umsetzung des IT-Sicherheitsfonds, insbesondere hinsichtlich der Mittelbereitstellung, institutionellen Verankerung und ersten Maßnahmen (vgl. Vorbemerkung der Fragesteller)?

4. Wie soll sichergestellt werden, dass flexible und strategisch einsetzbare Instrumente zur Verhinderung von Ausverkäufen, wie sie von der Bundesregierung im Strategiepapier angekündigt wurden (vgl. Bundestagsdrucksache 19/17296, S. 7), nicht mit dem EU-Beihilferecht oder den Wettbewerbsregeln in Konflikt geraten?
5. In welchen Fällen stützte sich die Bundesregierung seit Januar 2020 ggf. bei der Vergabe von Aufträgen auf die Ausnahmeregelung des § 12 der Verabreitung für die Bereiche Verteidigung und Sicherheit (VSVgV)?
6. Welche interministeriellen Abstimmungen oder Steuerungsmechanismen existieren ggf. bereits, um drohende Übernahmen von sicherheitsrelevanten Schlüsseltechnologien frühzeitig zu verhindern, bevor die Investitionsprüfmechanismen nach der AWV greifen?
7. Welche quantitativen Zielgrößen (z. B. Fondsvolumen, Anzahl der abzusichernden Technologien, Reaktionszeit bei drohenden Übernahmen) werden derzeit in den Planungen für die aktive Schutzstrategie diskutiert?
8. Wie weit konnte die Abhängigkeit von ausländischen Informationstechnologien nach Auffassung der Bundesregierung bislang reduziert werden, und welche Messgrößen werden hierfür herangezogen?

Berlin, den 25. November 2025

Dr. Alice Weidel, Tino Chrupalla und Fraktion