

## **Kleine Anfrage**

**der Abgeordneten Alexander Müller, Alexander Graf Lambsdorff, Grigorios Aggelidis, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Dr. Marco Buschmann, Dr. Marcus Faber, Otto Fricke, Katrin Helling-Plahr, Markus Herbrand, Manuel Höferlin, Ulla Ihnen, Olaf in der Beek, Dr. Marcel Klinge, Ulrich Lechte, Oliver Luksic, Dr. h. c. Thomas Sattelberger, Matthias Seestern-Pauly, Frank Sitta, Dr. Hermann Otto Solms, Katja Suding, Michael Theurer, Dr. Andrew Ullmann und der Fraktion der FDP**

### **Beschäftigung mit Deepfakes im Geschäftsbereich des Bundesministeriums der Verteidigung**

Die fortschreitende Digitalisierung hat längst schon in die militärische Domäne Einzug gehalten. In den letzten Jahren hat sich vor allem der Einsatz und der Einfluss von maschinellem Lernen, neuronalen Netzen und weiteren Bestandteilen „schwacher“ künstlicher Intelligenz massiv ausgeweitet. Im Zuge dessen spielen auch sog. Deepfakes (technisch manipulierte audiovisuelle Medien, die dazu geeignet sind, die Rezipierenden wirksam zu täuschen) eine immer größere Rolle. Die durch Deepfakes hervorgerufenen Gefahren im militärischen Bereich sehen die Fragestellenden vor allem im Bereich der hybriden Bedrohungen. Der Einsatz von Deepfakes bei Desinformationskampagnen oder zur Täuschung von Kommandoempfängern sind zwei Beispiele von denkbaren Anwendungsszenarien. Die Fragestellenden bewerten die bisherigen Auskünfte der Bundesregierung zur Beschäftigung mit Deepfakes im Verteidigungsbereich (siehe Bundestagsdrucksache 19/15657) als wenig aufschlussreich.

Wir fragen die Bundesregierung:

1. Welche Stellen bzw. Organisationselemente im Geschäftsbereich des Bundesministeriums der Verteidigung befassen sich mit der Thematik sog. Deepfakes?
2. Wie viele über den dienstlichen Meldeweg bekannt gewordene Vorgänge im Zusammenhang mit Deepfakes konnte die Bundeswehr in den letzten fünf Jahren zählen?
3. Welche Organisationselemente der Bundeswehr haben die Fähigkeit, Deepfakes zu erkennen?
4. Sind diese Organisationselemente mit der Befähigung zum Dienst rund um die Uhr ausgeplant?
5. Mit welchen Forschungseinrichtungen arbeitet der Geschäftsbereich des Bundesministeriums der Verteidigung bei der Erkennung von Deepfakes und der Forschung dazu zusammen?

6. Befasst sich der Geschäftsbereich des Bundesministeriums der Verteidigung mit Deepfakes als Mittel zur Manipulation der militärischen Befehlskette?
7. Hat die Bundeswehr bereits Strategien zur Detektion und zum Umgang mit Deepfakes?  
Welche Organisationselemente werden dabei eingebunden?
8. Welche Rollen spielen der Presse- bzw. Informationsstab des Bundesministeriums der Verteidigung und die für die Informationsarbeit zuständigen Organisationselemente der Bundeswehr beim Umgang mit Deepfakes?
9. Wie thematisiert das Bundesministerium der Verteidigung Deepfakes im strategischen Kontext?
10. Zieht die Bundesregierung die Teilnahme an Wettbewerben oder Ähnlichem (Beispiel: Deepfake Detection Challenge) mit Teams der Bundeswehr in Betracht?
11. Welche Projekte, die die Thematik Deepfakes betreffen, werden im Cyber Innovation Hub der Bundeswehr durchgeführt?

Berlin, den 26. Februar 2020

**Christian Lindner und Fraktion**