Landtag von Baden-Württemberg **Drucksache 17 / 2938**

17. Wahlperiode **21.7.2022**

Kleine Anfrage

des Abg. Jonas Hoffmann SPD

und

Antwort

des Ministeriums des Inneren, für Digitalisierung und Kommunen

Umgang mit Deepfakes und Bildmanipulationen in Baden-Württemberg

Kleine Anfrage

Ich frage die Landesregierung:

1. Wie viele Fälle welcher Art von Deepfakes bzw. Bildmanipulationen in Baden-Württemberg sind der Landesregierung bekannt?

2. Welche strafrechtlichen Möglichkeiten gibt es, um gegen Deepfakes bzw. Bildmanipulationen vorzugehen?

3. In welchen Bereichen entstehen konkrete Gefahren, die von Deepfakes bzw. Bildmanipulationen ausgehen?

4. Welche Erkenntnisse liegen ihr zur Beeinflussung von politischen Prozessen durch Deepfakes bzw. Bildmanipulationen vor?

5. Welche Möglichkeiten bieten Deepfakes bzw. Bildmanipulationen, um Desinformationen zu verbreiten?

6. Wie wirkt sie Desinformation durch Deepfakes bzw. Bildmanipulationen entgegen?

7. In welcher Form beschäftigt sich die Cybersicherheitsagentur mit dem Thema Deepfakes bzw. Bildmanipulationen, unter Darstellung, ob es eine Abteilung gibt, die sich schwerpunktmäßig mit dem Betrug durch Deepfakes bzw. Bildmanipulationen beschäftigt?

8. Welche Maßnahmen ergreift die Landesregierung, um Bürgerinnen und Bürger, aber auch Einrichtungen des Landes oder der Kommunen vor Deepfakes bzw. Bildmanipulationen zu schützen, unter Darstellung, an welche Stelle sich Betroffene wenden können?

Eingegangen: 21.7.2022 / Ausgegeben: 29.8.2022

9. Wurden der Ministerpräsident, die weiteren Mitglieder der Landesregierung und kommunale Entscheidungsträger im Umgang mit Deepfakes bzw. Bildmanipulationen geschult?

10. Welchen Handlungsbedarf sieht sie beim Thema Deepfakes bzw. Bildmanipulationen?

21.7.2022

Hoffmann SPD

Begründung

Die Bürgermeisterin von Berlin sowie die Bürgermeister von Wien und Madrid sind in Videoanrufen einem falschen Klitschko gegenübergetreten. Vor dem Hintergrund dieser Ereignisse stellt sich die Frage, wie beispielsweise der Ministerpräsident im Umgang mit Bildmanipulation bzw. Deepfakes geschult ist. Insgesamt soll die Kleine Anfrage in Erfahrung bringen, wie das Thema der Bildmanipulationen bzw. Deepfakes in Baden-Württemberg behandelt wird und welche Erkenntnisse hierzu vorliegen.

Antwort

Mit Schreiben vom 16. August 2022 Nr. IM3-0141.5-240/72/5 beantwortet das Ministerium des Inneren, für Digitalisierung und Kommunen die Kleine Anfrage wie folgt:

1. Wie viele Fälle welcher Art von Deepfakes bzw. Bildmanipulationen in Baden-Württemberg sind der Landesregierung bekannt?

Zu 1.:

Die statistische Erfassung von Straftaten erfolgt bei der Polizei Baden-Württemberg anhand der Polizeilichen Kriminalstatistik (PKS). Bei der PKS handelt es sich um eine sogenannte reine Ausgangsstatistik, in der strafrechtlich relevante Sachverhalte nach der polizeilichen Sachbearbeitung vor Abgabe an die Strafverfolgungsbehörden erfasst werden. Die Fallerfassung erfolgt nach den bundeseinheitlichen „Richtlinien für die Führung der Polizeilichen Kriminalstatistik“. Eine statistische Erhebung von Straftaten unter Verwendung von Deepfakes oder Bildmanipulationen erfolgt hierbei nicht.

Der Cyberabwehr des Landesamtes für Verfassungsschutz Baden-Württemberg (LfV) sowie der Cybersicherheitsagentur Baden-Württemberg (CSBW) liegen hierzu ebenfalls keine Fallzahlen vor.

2. Welche strafrechtlichen Möglichkeiten gibt es, um gegen Deepfakes bzw. Bildmanipulationen vorzugehen?

Zu 2.:

Die Erstellung sogenannter Deepfakes sowie die Vornahme von Bildmanipulationen sind als solche nicht strafbar. Für eine Strafbarkeit entscheidend ist die Art der Verwendung im konkreten Einzelfall. Grundsätzlich kommen Deepfakes

und Bildmanipulationen bei zahlreichen Delikten als Tatmittel in Betracht. Sofern durch die Art der Verwendung der Anfangsverdacht auf eine verfolgbare Straftat besteht, stehen die jeweils einschlägigen Maßnahmen der Strafprozessordnung zur Ermittlung und strafrechtlichen Verfolgung der Täter zur Verfügung.

3. In welchen Bereichen entstehen konkrete Gefahren, die von Deepfakes bzw. Bildmanipulationen ausgehen?

Zu 3.:

Ein mögliches Anwendungsfeld ist das sogenannte „Social Engineering“, bei dem Täter versuchen, Personen – insbesondere aus dem politischen oder wirtschaftlichen Bereich – durch Täuschung zu beeinflussen, um ein bestimmtes Verhalten herbeizuführen. Dabei kann es sich beispielsweise um die Installation von Schadsoftware, die Herausgabe sensibler Informationen oder auch die Freigabe von Finanzmitteln handeln. Deepfakes und Bildmanipulationen sind zudem dazu geeignet, Personen zu diskreditieren oder mit der Drohung einer Veröffentlichung zu erpressen.

Im politischen Bereich und in der öffentlichen Verwaltung besteht zudem die Gefahr von Desinformationskampagnen, die auf die Beeinflussung der öffentlichen Meinungsbildung abzielen. Derartige Aktivitäten können beispielsweise zur illegitimen Einflussnahme auf Wahlen oder aktuell zur propagandistischen Unterstützung der militärischen Aggression gegen die Ukraine eingesetzt werden.

4. Welche Erkenntnisse liegen ihr zur Beeinflussung von politischen Prozessen durch Deepfakes bzw. Bildmanipulationen vor?

Zu 4.:

Diesbezüglich liegen keine konkreten Erkenntnisse vor. Zu der in der Begründung der Kleinen Anfrage genannten Videokonferenz zwischen der Bürgermeisterin von Berlin und einem angeblichen Vitali Klitschko liegen dem LfV keine Hinweise auf einen nachrichtendienstlichen oder staatlichen Hintergrund vor. Es ist jedoch nicht auszuschließen, dass ausländische Nachrichtendienste oder staatlich gesteuerte Akteure Deepfakes zukünftig als weiteres Angriffs- oder Desinformationsmittel nutzen könnten.

5. Welche Möglichkeiten bieten Deepfakes bzw. Bildmanipulationen, um Desinformationen zu verbreiten?

Zu 5.:

Durch einen Deepfake oder eine Bildmanipulation ist es möglich, glaubwürdige Falschinformationen zu verbreiten, indem manipulierte Medieninhalte von Schlüsselpersonen erzeugt und verbreitet werden. Da von einer zeitnahen Richtigstellung der betroffenen Stellen auszugehen ist, bieten derartige Aktionen eher die Möglichkeit zur kurzzeitigen Desinformation.

6. Wie wirkt sie Desinformation durch Deepfakes bzw. Bildmanipulationen entgegen?

7. In welcher Form beschäftigt sich die Cybersicherheitsagentur mit dem Thema Deepfakes bzw. Bildmanipulationen, unter Darstellung, ob es eine Abteilung gibt, die sich schwerpunktmäßig mit dem Betrug durch Deepfakes bzw. Bildmanipulationen beschäftigt?

8. Welche Maßnahmen ergreift die Landesregierung, um Bürgerinnen und Bürger, aber auch Einrichtungen des Landes oder der Kommunen vor Deepfakes bzw. Bildmanipulationen zu schützen, unter Darstellung, an welche Stelle sich Betroffene wenden können?

9. Wurden der Ministerpräsident, die weiteren Mitglieder der Landesregierung und kommunale Entscheidungsträger im Umgang mit Deepfakes bzw. Bildmanipulationen geschult?

10. Welchen Handlungsbedarf sieht sie beim Thema Deepfakes bzw. Bildmanipulationen?

Zu 6. bis 10.:

Die Fragen werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Durchführung manipulierter Videokonferenzen, wie beispielsweise die in der Begründung genannte Videokonferenz zwischen der Bürgermeisterin von Berlin und einem angeblichen Vitali Klitschko, basiert auf „Social Engineering“. Bei potenziell von Deepfakes oder Bildmanipulation betroffenen Stellen kann auf längerfristige Sicht daher eine entsprechende Sensibilisierung in Bezug auf „Social Engineering“ eine wirksame Gegenmaßnahme darstellen. Eine kurzfristige Gegenmaßnahme kann zudem eine „Zwei-Faktoren-Authentifizierung“ sein, bei der vor Beginn einer Videokonferenz zum Bespiel mit der Pressestelle des vermeintlichen Gesprächspartners Rücksprache gehalten wird. Während der Videokonferenz selbst kann auf Anzeichen für einen Deepfake oder eine Bildmanipulation geachtet werden. Dabei handelt es sich beispielsweise um eine fehlende Synchronität von Lippen und Sprache, ruckartige Bewegungen oder plötzliche Änderung der Belichtung.

Der CSBW obliegt – neben den vielfältigen Aufgaben zum Schutz der öffentlichen Stellen vor Cyberangriffen – auch der Schutz gesellschaftlich relevanter Prozesse im Cyberraum nach § 3 Absatz 1 Ziffer 2 Cybersicherheitsgesetz Baden-Württemberg. In diesem Kontext wurden etwa anlässlich der Bundestagswahl gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) mögliche Maßnahmenempfehlungen geprüft, abgestimmt und als Handlungsempfehlungen den Kommunen zur Verfügung gestellt. Im Fokus standen hierbei jedoch vor allem allgemeine Themen der IT- und Informationssicherheit auf Basis der Standards des BSI. Als eine spezielle Maßnahme zur Vermeidung von Fake News bei der letzten Bundestagswahl wurde den Kandidierenden über die Landeswahlleitung in Abstimmung mit dem BSI konkrete Hinweise gegeben, wie die jeweiligen Social-Media-Accounts verifiziert werden können, sodass Abonnenten der Accounts, also die Bürgerinnen und Bürger, Gewähr haben, dass die von den Accounts veröffentlichten Beiträge auch authentisch sind.

Die potenziellen Gefährdungen durch Deepfakes und Bildmanipulationen werden in verschiedenen Abteilungen der CSBW aktuell aufgegriffen, so etwa unter dem Gesichtspunkt der Schulungen und Sensibilisierung. Die CSBW wird im Rahmen ihres E-Learning-Angebots auch ein Kapitel zum Thema Deepfakes erarbeiten und bereitstellen. Zudem werden die als relativ neu zu bezeichnenden Herausforderungen künftig auch in der Sensibilisierungskampagne der CSBW zu Themen der Cybersicherheit Niederschlag finden.

Angriffe auf die Demokratie durch Fake News, Propaganda oder Desinformation, die geeignet sind, Hass und Angst zu schüren, wurden im Koalitionsvertrag der Landesregierung 2021 bis 2026 aufgegriffen und in der Folge der Kabinettsausschuss „Entschlossen gegen Hass und Hetze“ eingerichtet. Neben den mitwirkenden Ressorts hat auch die Task Force gegen Hass und Hetze unter Federführung des Landeskriminalamts Baden-Württemberg (LKA) ihre Arbeit aufgenommen. Ihre Aufgabe ist es, einschlägige Bedrohungen im Bereich Hass und Hetze festzustellen und ihnen entgegenzuwirken. Ein besonderes Augenmerk wird dabei auf Prävention und die Stärkung der Medienkompetenz bereits in der Schule gelegt. Als ein erstes Ergebnis ist die Website der Initiative Toleranz im Netz (*www.initiative-toleranz-im-netz.de*) entstanden. Diese stellt umfangreiche Informationen und Unterstützung für Betroffene von Hasskriminalität sowie für interessierte Personen bereit, wie beispielsweise passende Ansprechstellen, Möglichkeiten zur Meldung von Hass und Hetze oder zur Anzeigeerstattung oder Angebote aus dem Bereich des Opferschutzes. Daneben können verschiedene Zielgruppen zu unterschiedlichen Bildungsangeboten Kontaktmöglichkeiten finden.

Informationen über Risiken und Konsequenzen von Deepfakes und Bildmanipulationen sind darüber hinaus regelmäßig Bestandteil von Präventionsveranstaltungen der Polizei Baden-Württemberg im Themenfeld Digitale Sicherheit für Bürgerinnen und Bürger verschiedener Altersgruppen. Betroffene werden zudem beraten, wie mit entsprechenden Inhalten umgegangen werden kann. Die polizeilichen Präventionsangebote unterliegen einem kontinuierlichen Monitoring- und Aktualisierungsprozess. Dies gilt insbesondere für dynamische Handlungsfelder wie Deepfakes und Bildmanipulationen. Auf neu auftretende Tatbegehungs- und Verbreitungsphänomene wird gegebenenfalls unmittelbar mit zielgruppenorientierten Informations- und Sensibilisierungsmaßnahmen reagiert.

Auf der Internet-Seite *www.polizei-beratung.de* des bundesweiten polizeilichen Vorbeugungsprogramms sind weitere themenzentrierte Informationen zu den Themen „Deepfake“ und „Video- und Bildmanipulation“ verfügbar, auf die im Rahmen der präventiven Öffentlichkeitsarbeit hingewiesen wird.

Das LKA hat zudem ein Vortragskonzept entwickelt, welches sich gezielt an Amts- und Mandatsträgerinnen und -träger richtet und unter anderem über sicherheitsbewusstes Verhalten in der Öffentlichkeit informiert. Ein wichtiger Aspekt ist dabei die Sensibilisierung im Umgang mit sozialen Medien und sensiblen persönlichen Daten.

Die Cyberabwehr des LfV bearbeitet auf der Grundlage des Gesetzes über den Verfassungsschutz in Baden-Württemberg (Landesverfassungsschutzgesetz) Cyber-Angriffe mit (mutmaßlich) nachrichtendienstlichem Hintergrund. Im Rahmen dieses gesetzlichen Auftrags steht das LfV grundsätzlich als Ansprechpartner im Land zur Verfügung und kann anlassbezogen wie anlassunabhängige Präventions- und Sensibilisierungsmaßnahmen für Politik, Verwaltung und potenziell betroffene Wirtschaftsunternehmen durchführen.

In Vertretung

Klenk

Staatssekretär