Landtag von Baden-Württemberg **Drucksache 17 / 8433**

17. Wahlperiode **21.2.2025**

Kleine Anfrage

des Abg. Dr. Stefan Fulst-Blei SPD

und

Antwort

des Ministeriums des Inneren, für Digitalisierung und Kommunen

Gefahrenpotenzial von Fake News mit Blick auf die anstehenden Landtagswahlen

Kleine Anfrage

Ich frage die Landesregierung:

1. Gab es in Baden-Württemberg Fälle oder Vorkommnisse, bei denen in den letzten drei Jahren Fake News (hier gemeint im engeren Sinne von falschen Nachrichtenmeldungen – nicht Fake-Profile auf Social Media, Enkel-Trickbetrugsmasche o. Ä.) gezielt zur Täuschung von Privatpersonen, politischen Akteuren, Organisationen oder Unternehmen eingesetzt wurden?

2. Welche Gefahren sieht sie mit Blick auf die mögliche Einflussnahme durch künstliche Intelligenz und Fake News auf die Landespolitik in Baden-Württemberg?

3. Sind ihr Vorfälle von Videoverfälschung mit Landespolitikerinnen und Landespolitikern bekannt, falls ja, welche?

4. Sind ihr Vorfälle von Stimmenimitationen auf Grundlage von künstlicher Intelligenz mit Landespolitikerinnen und Landespolitikern bekannt, falls ja, welche?

5. Wie schätzt sie die technischen Potenziale zur Erstellung entsprechender Fakes ein?

6. Welche Vorfälle mit Verfälschungen sprachbasierter beziehungsweise bildbasierter Fakes im Bundestagswahlkampf sind ihr mit Blick auf Politikerinnen und Politiker aus dem Land Baden-Württemberg bislang bekannt geworden?

7. Wie schätzt sie die Gefahr zur Einflussnahme im Landtagswahlkampf 2026 ein?

Eingegangen: 21.2.2025 / Ausgegeben: 25.3.2025

8. Welche Erkenntnisse hat die Landesregierung aus den Einflussnahmen aus dem aktuellen Bundestagswahlkampf gewonnen und inwiefern führen diese Erkenntnisse zu Vorsichtsmaßnahmen und Schutzmaßnahmen hinsichtlich des Landtagswahlkampfs 2026?

21.2.2025

Dr. Fulst-Blei SPD

Begründung

Die aktuelle Bundestagswahl zeigt, welch großen Einfluss Informationen aus dem Internet auf die Wahlentscheidung von Wählerinnen und Wählern haben. Nicht immer sind diese Informationen vertrauenswürdig, teils sogar Fake News, um gezielt Menschen zu beeinflussen und zu verunsichern. In Rumänien wurden sogar Wahlen annulliert aufgrund von Fake News. Angesichts dieser Gefahrenpotenziale für unsere Demokratie soll diese Kleine Anfrage die aktuelle Situation in Baden-Württemberg mit Blick auf die anstehende Landtagswahl ergründen.

Antwort

Mit Schreiben vom 19. März 2025 Nr. IM6-0141.5-664/3/5 beantwortet das Ministerium des Inneren, für Digitalisierung und Kommunen die Kleine Anfrage wie folgt:

1. Gab es in Baden-Württemberg Fälle oder Vorkommnisse, bei denen in den letzten drei Jahren Fake News (hier gemeint im engeren Sinne von falschen Nachrichtenmeldungen – nicht Fake-Profile auf Social Media, Enkel-Trickbetrugsmasche o. Ä.) gezielt zur Täuschung von Privatpersonen, politischen Akteuren, Organisationen oder Unternehmen eingesetzt wurden?

Zu 1.:

Das Landesamt für Verfassungsschutz Baden-Württemberg (LfV) beobachtet Desinformation als Instrument fremdstaatlicher Einflussnahme im Sinne des § 3 Absatz 2 Satz 1 Nummer 2 Landesverfassungsschutzgesetz (LVSG) oder Mittel extremistischer Bestrebungen im Sinne des § 3 Absatz 2 Satz 1 Nummer 1, 3, 4 LVSG. Eine verfassungsschutzseitige Zuständigkeit besteht mithin nur, wenn sich Desinformation als politisch bestimmte, ziel- und zweckgerichtete Verhaltensweise oder als Teil geheimdienstlicher Tätigkeiten für eine fremde Macht gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richtet.

Unter dem Begriff Desinformation versteht das LfV – in Abgrenzung zu den Begriffen der Falschinformation, Malinformation oder „Fake News“ – die absichtlich-manipulative und zielgerichtete Verbreitung objektiv unzutreffender, irreführender oder in wesentlichen Teilen unvollständiger Inhalte. Der Begriff „Fake News“ findet im Verfassungsschutzkontext keine Verwendung.

Eine Quantifizierung aller Fälle von Desinformation der letzten drei Jahre ist vor dem Hintergrund der Masse an einschlägigen Inhalten, insbesondere im digitalen Informationsraum, nicht möglich. Desinformation ist zudem regelmäßig auf einen überregionalen oder gar internationalen Wirkkreis ausgelegt, sodass einer Begrenzung auf Vorkommnisse in Baden-Württemberg nur geringe Aussagekraft zu-

kommt. Spätestens seit Beginn des russischen Angriffskriegs gegen die Ukraine im Jahr 2022 ist die Russische Föderation als einer der zentralen Emittenten von Desinformation in Deutschland und Baden-Württemberg zu benennen. Exemplarisch sei hier auf die unter anderem vor der Bundestagswahl 2025 in den sozialen Medien aktive Kampagne „Doppelgänger“ verwiesen. Hier wurden gefälschte Nachrichten verbreitet, um westliche Regierungen, insbesondere im Kontext des Ukrainekrieges zu diskreditieren. Dafür wurden Imitationen seriöser Medienseiten, inauthentische und automatisierte Social-Media-Accounts sowie selbst erstellte Nachrichten-Portale eingesetzt. Beispielhaft erwähnt werden kann zudem auch die ebenfalls vor der Bundestagswahl aktive „Matryoshka“-Kampagne, welche durch massenhafte Meldung gefälschter, zuvor selbst erstellter Social-Media-Inhalte, auf eine Überlastung von Fakten-Checkern, Wissenschaftlern, Medienverantwortlichen und Journalisten abzielte.

2. Welche Gefahren sieht sie mit Blick auf die mögliche Einflussnahme durch künstliche Intelligenz und Fake News auf die Landespolitik in Baden-Württemberg?

Zu 2.:

Wenngleich die strategischen Interessen fremdstaatlicher Einflussnahme häufig im Bereich der Bundespolitik liegen, können politische Prozesse auf Landesebene einen Hebel zur Verschiebung innenpolitischer Machtverhältnisse sowie eine Möglichkeit zur Schwächung des gesellschaftlichen Zusammenhalts und Vertrauens in den Staat darstellen. Desinformation ist zudem potenziell Mittel extremistischer Mobilisierung. Schließlich kann es im Bereich der Informationsmanipulation auch zum Zusammenwirken fremdstaatlicher und extremistischer Akteure kommen. So nutzte die Russische Föderation in der Vergangenheit rechtsextremistische Influencer zur Beeinflussung demokratischer Wahlen.

Für die politische Ausrichtung Baden-Württembergs stellen insbesondere Landtagswahlen einen neuralgischen Punkt illegitimer Einflussnahme und extremistischer Agitation dar. Desinformation soll in diesem Kontext Kräfte des demokratischen Parteienspektrums diskreditieren, Konflikte anheizen, Menschen einschüchtern und Vertrauen zerstören. Die Nutzung von Künstlicher Intelligenz (KI) ermöglicht ein erhebliches Wachstum des quantitativen Outputs bei gleichzeitiger Steigerung des qualitativen Täuschungspotenzials manipulativer Inhalte. Selbst bei zeitnah entkräfteter Desinformation („Debunking“) oder offensichtlich KI-generierten Inhalten können nachhaltige Wirkeffekte eintreten („continued influence effect“). Sowohl die breitflächige Kontaminierung des Informationsraums als auch gezielte Desinformations-Operationen vermögen es, langfristig Entfremdung und Desintegration im Verhältnis zwischen Bevölkerung und Landespolitik hervorzurufen.

In Baden-Württemberg verbreiten rechtsextremistische Organisationen und Gruppierungen regelmäßig KI-generierte Bilder, Memes und sonstigen Content, von den Parteien AfD (Verdachtsfall des LfV) und „Die Heimat“ über die Gruppierung „Pforzheim Revolte“ bis hin zu „Reconquista 21“ (R21), Teilorganisation der „Identitären Bewegung Deutschland e. V.“ (IBD). Insgesamt beschränkt sich der proaktive Einsatz von KI durch die entsprechenden Akteure nach derzeitigem Kenntnisstand aber auf ein noch überschaubares Maß. Es ist jedoch zu erwarten, dass rechtsextremistische Akteure den Einsatz von KI in Zukunft intensivieren werden. Verschiedene Tools bieten den Vorteil, dass der Aufwand rund um die Content-Produktion gesenkt werden kann. Auch dürfte der Einsatz von KI eine Geldersparnis darstellen, indem zum Beispiel grafisch ansprechende Flyer selbst statt durch Agenturen beziehungsweise Druckereien erstellt werden. Nicht zuletzt profitieren rechtsextremistische Akteure generell von einem öffentlichkeitswirksamen Auftritt, der ästhetisch zeitgemäß ist und damit die Anknüpfungsfähigkeit aufrechterhält.

Im Ergebnis ist daher davon auszugehen, dass rechtsextremistische Akteure von KI erstellte oder manipulierte Inhalte für sich zu nutzen wissen und diese in Zukunft vermehrt zur Verbreitung und Umsetzung ihrer verfassungsfeindlichen Ziele einsetzen werden. Damit einher geht die Möglichkeit, dass KI auch verwendet werden kann, um die Landespolitik zu delegitimieren bzw. Landespolitikerinnen und Landespolitiker anzugreifen und ihnen auf diese Weise zu schaden.

Innerhalb der Szene der „Reichsbürger und Selbstverwalter“ sowie der „Verfassungsschutzrelevanten Delegitimierung des Staates“ wird KI bislang eher als Bedrohung angesehen, zum Beispiel im Zusammenhang mit dem vermeintlichen Einsatz als Überwachungsinstrument des Staates. Dennoch ist zu erwarten, dass auch in diesen Milieus in Zukunft der Einsatz von KI zunehmen wird, beispielsweise zur professionelleren Gestaltung und einfacheren Verbreitung der eigenen Propaganda. Fake News und Desinformation werden innerhalb dieser Milieus bislang eher selten selbst produziert. Allerdings ist eine umfangreiche Verbreitung entsprechender Inhalte zu beobachten. „Reichsbürger“ und Staatsdelegitimierer fungieren dadurch bislang eher als Multiplikatoren von Fake News und Desinformation.

Hinsichtlich des Bereichs „Islamistischer Extremismus und Terrorismus“ wird auf die Antwort zu Frage 5 verwiesen. In anderen Phänomenbereichen, wie dem Linksextremismus, kommt der Verbreitung von Desinformation durch KI-generierte Inhalte bislang keine größere Bedeutung zu.

3. Sind ihr Vorfälle von Videoverfälschung mit Landespolitikerinnen und Landespolitikern bekannt, falls ja, welche?

4. Sind ihr Vorfälle von Stimmenimitationen auf Grundlage von künstlicher Intelligenz mit Landespolitikerinnen und Landespolitikern bekannt, falls ja, welche?

Zu 3. und 4.:

Die Fragen 3 und 4 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet. Es liegen keine Erkenntnisse zu Vorfällen im Sinne der Fragestellungen vor.

5. Wie schätzt sie die technischen Potenziale zur Erstellung entsprechender Fakes ein?

Zu 5.:

Emittenten von Desinformation nutzen KI sowohl zur inhaltlichen Gestaltung von Beiträgen (z. B. Bild-, Video-, Audio- und Textgenerierung) als auch zu deren formaler Erstellung (z. B. Übersetzung in die Zielsprache) und Verbreitung (z. B. automatisierte Bot-Netzwerke, synthetische Accounts). Ferner ermöglicht die KI-gestützte Sammlung und Auswertung von Massendaten (z. B. Nutzerdaten in den sozialen Medien) eine genauere Anpassung manipulativer Inhalte an tagesaktuelle Trends sowie an Denk- und Verhaltensmuster des jeweiligen Zielpublikums.

Kurz- bis mittelfristig ist damit zu rechnen, dass KI-generierte Bilder, Videos, Audioaufnahmen und Texte schwerer als solche zu erkennen sind, das Verhalten von Bot-Netzwerken oder synthetischen Accounts zunehmend dem Agieren menschlicher Internetnutzer gleicht und personalisierte Desinformation zielgenauer an den jeweiligen Adressatenkreis gelangt. Das quantitative und qualitative Gefahrenpotenzial durch manipulative Informationen dürfte vor diesem Hintergrund eine erhebliche Steigerung erfahren.

Prinzipiell bieten die technischen Voraussetzungen und ihre niedrigschwellige Zugänglichkeit auch extremistischen Gruppierungen (Islamistischer Extremismus und Terrorismus) die Möglichkeit zur Erstellung von Desinformation. Außer KI-generierten Bildern zur Agitation im Zusammenhang mit dem Nahostkonflikt haben Islamisten dieses Aktionsfeld jedoch noch nicht für sich entdeckt.

Bei rechtsextremistischen Akteuren ist wesentlich häufiger zu beobachten, dass sie KI-generierte Inhalte von bundesweit oder anderweitig verorteten Aktivisten bzw. Multiplikatoren teilen, anstatt selbst Content zu kreieren. Auf diese Weise erfahren Desinformationen weite Verbreitung und werden in das ideologische Weltbild der Extremisten eingewoben. Nichtsdestotrotz sind auch rechtsextremistische Akteure in der Lage, professionelle Desinformation mit oder ohne KI zu generieren. Mittlerweile gibt es im Bereich Rechtsextremismus mehrere Kommunikations- und Medienagenturen, die teilweise „Künstliche Intelligenz“ zu ihrem Portfolio zählen.

In anderen Phänomenbereichen wie dem Linksextremismus kommt der Verbreitung von Desinformation durch KI-generierte Inhalte bislang keine größere Bedeutung zu. Im Übrigen wird auf die Antwort zu Frage 2 verwiesen.

6. Welche Vorfälle mit Verfälschungen sprachbasierter beziehungsweise bildbasierter Fakes im Bundestagswahlkampf sind ihr mit Blick auf Politikerinnen und Politiker aus dem Land Baden-Württemberg bislang bekannt geworden?

Zu 6.:

Im Bundestagswahlkampf wurden keine Vorfälle von Verfälschungen sprachbasierter beziehungsweise bildbasierter Fakes mit Blick auf Politikerinnen und Politiker aus Baden-Württemberg bekannt.

7. Wie schätzt sie die Gefahr zur Einflussnahme im Landtagswahlkampf 2026 ein?

Zu 7.:

Im Rahmen der Bundestagswahl 2025 wurden deutschlandweit Fälle von Einflussnahme, mehrheitlich durch russische Akteure, festgestellt. Diese umfassten vor allem Desinformationskampagnen im digitalen Raum, meist unter Nutzung von sozialen Medien. Dabei wurden Beiträge mit Desinformation eingestellt und sowohl von realen Profilen, zum Beispiel bezahlten Influencern, aber auch von automatisierten Profilen, sogenannten „Social Bots“, verbreitet. Im analogen Raum beobachtet das LfV Fälle von „Low-level-Agents“, also Personen, die ohne eigene Zugehörigkeit gegen Bezahlung Dienste für ausländische Nachrichtendienste leisten – zum Beispiel zur Spionage oder zur Vorbereitung oder Durchführung von Sabotageaktivitäten.

Die Wahrscheinlichkeit von Einflussnahmeaktivitäten und Desinformationskampagnen im Landtagswahlkampf 2026 ist deshalb hoch. Ausländische Einflussnahmeakteure, wie die russischen Akteure „Matryoshka“ und „Doppelgänger“ haben bewiesen, dass sie trotz des kurzfristig angesetzten Wahltermins quantitativ umfassend und qualitativ hochwertig aktiv werden können. Die offensichtlich stark ausgeprägte Nutzung von KI-generierten Bildern und Videos, zum Teil unter Einsatz von Schauspielern, deren Gesichter abgewandelt wurden („Defacement“), und der Einsatz staatsnaher Akteure, wie beispielsweise der „Prankster“ „Vovan und Lexus“ können ohne großen finanziellen und personellen Aufwand zur Wirkung gebracht werden. „Vovan und Lexus“ beispielsweise sind mindestens seit 2022 in weitreichende Einflusskampagnen Russlands involviert und dafür bekannt, mit Telefon- und Videoanrufen unter falscher Identität (u. a. Deepfakes) westliche Politikerinnen und Politiker in die Irre zu führen. Bei „Vovan und Lexus“ ist zu vermuten, dass sie ihre Aktionen mit Zustimmung und Unterstützung staatlicher russischer Stellen durchführen. Sie können daher als zumindest staatlich geduldete Einflussakteure betrachtet werden (weitere Informationen abrufbar unter *https://www.verfassungsschutz-bw.de/,Lde/Startseite/Meldungen+und+Archiv/Prank-Anrufe+russischer+Akteure*).

Wenngleich ausländische Einflussnahmeakteure nahezu sicher verstärkt auf gesamtstaatliche Wahlen abzielen, sind Aktivitäten auch im baden-württembergischen Landtagswahlkampf wahrscheinlich. Dies ist darauf zurückzuführen, dass Baden-Württemberg aufgrund seiner wirtschaftlichen, wissenschaftlichen und politischen Bedeutung zumindest auch im Fokus ausländischer Staaten steht. Zudem haben die Akteure bewiesen, dass sie schnell und kurzfristig ihren Fokus ändern können, dass ihre Methoden etabliert sind und aufgrund der Nutzung von KI-basierten Ansätzen kostengünstig zum Einsatz kommen können.

Im Bereich der Cyberabwehr stellen Phishing-Angriffe häufig den Ausgangspunkt für Cyberspionage- oder Cybersabotageangriffe dar. Mit diesen Angriffen gehen zu Beginn einer Attacke oftmals ausgefeilte manipulative Methoden („Social Engineering“) einher, um Menschen zu einem bestimmten, sicherheitskritischen Verhalten zu verleiten. Außerdem verwenden Angreifer vielfach sogenannte Spear-Phishing-E-Mails, die passgenau auf die Interessenlagen weniger Empfänger oder Einzelpersonen zugeschnitten sind, um zum Beispiel mittels versteckt integrierter oder angehängter Schadsoftware IT-Systeme zu kompromittieren und so letztlich unbemerkt Datenabflüsse zu generieren.

Daneben sind auch Hack-and-Leak- beziehungsweise Hack-and-Publish-Angriffe nicht auszuschließen. Bei einem Hack-and-Leak-Angriff werden legitime Nachrichtenportale oder Social-Media-Auftritte gezielt gehackt, um anschließend Informationen im Original – oder verfälscht – zu veröffentlichen. Hack-and-Publish-Angriffe werden dazu verwendet, legitime Internetseiten zu kompromittieren und Inhalte zum Zweck der Desinformation zu veröffentlichen. Ein solches Angriffsziel könnten etwa Internetseiten sein, auf denen das offizielle Wahlergebnis veröffentlicht wird, um das Vertrauen der Bevölkerung in die Legitimität des Wahlprozesses zu erschüttern.

Ausländische Staaten setzen dabei für Angriffe im Cyberraum verschiedene Cybergruppierungen ein. Diese werden generell als APT-Gruppe („Advanced Persistent Threat“, „fortgeschrittene, andauernde Bedrohung“) bezeichnet und sollen die wahre Identität von Angriffen verschleiern. APT-Angriffe zeichnen sich durch einen sehr hohen personellen wie finanziellen Ressourceneinsatz sowie erhebliche technisch-methodische Fähigkeiten aus und sind nur sehr schwer zu entdecken. Mit diesen Angriffen gehen zu Beginn einer Attacke oftmals ausgefeilte manipulative Methoden (Social Engineering) einher, um Menschen zu einem bestimmten sicherheitskritischen Verhalten zu verleiten. Außerdem verwenden APT vielfach sogenannte Spear-Phishing-E-Mails, die passgenau auf die Interessenlagen weniger Empfänger oder Einzelpersonen zugeschnitten sind, um zum Beispiel mittels versteckt integrierter oder angehängter Schadsoftware IT-Systeme zu kompromittieren und so letztlich unbemerkt Datenabflüsse zu generieren. Im Kontext von möglichen Cyberangriffen mit Bezug auf die Landtagswahl 2026 kann hier beispielhaft die APT-Gruppe „Ghostwriter“ genannt werden. Diese ist seit mindestens 2016 aktiv und wird nahezu sicher dem russischen Staat und konkret dem russischen Militärgeheimdienst GRU zugeordnet.

8. Welche Erkenntnisse hat die Landesregierung aus den Einflussnahmen aus dem aktuellen Bundestagswahlkampf gewonnen und inwiefern führen diese Erkenntnisse zu Vorsichtsmaßnahmen und Schutzmaßnahmen hinsichtlich des Landtagswahlkampfs 2026?

Zu 8.:

Nach Einschätzung des Verfassungsschutzes kam es im Vorfeld der Bundestagswahl 2025 zu verstärkten Versuchen der illegitimen Einflussnahme auf den deutschen Diskurs- und Informationsraum. Festgestellt wurden sowohl die Verbreitung von teils KI-gestützter Desinformation als auch die gezielte Verdichtung negativer Berichterstattung zu gesellschaftlichen Konflikten und Reizthemen. Die in der Regel ideologisch flexible Verstärkung bestehender Ressentiments soll Konflikte anheizen, Menschen einschüchtern und Vertrauen zerstören. Entscheidend ist dabei das Schadpotenzial eines Themas, weniger das Thema selbst.

Der Verfassungsschutzverbund hatte aufgrund des zu erwartenden Umfangs ausländischer Einflussnahmeaktivitäten für den Zeitraum des Bundestagswahlkampfs 2025 eine Sonderauswertung (SAW) eingerichtet. Das LfV schloss sich dieser SAW an. Sowohl in Bezug auf inhaltlich-fachliche Fragestellungen als auch in Bezug auf die organisatorischen Abläufe und die Zusammenarbeit mit den maßgeblich beteiligten Stellen in Bund und Land konnten hieraus wertvolle Erkenntnisse gewonnen werden. Diese werden in einem internen, eingestuften Abschlussbericht erfasst und für die Gewährleistung der Sicherheit der Landtagswahlen nutzbar gemacht.

Beispielhaft für Maßnahmen, die sowohl im Bundestagswahlkampf 2025 als auch im Landtagswahlkampf 2026 getroffen werden, ist die Onlineveranstaltung „Sicher im Wahlkampf“ zu nennen. Dieses vom Landeskriminalamt Baden-Württemberg (LKA BW) gemeinsam mit der Cybersicherheitsagentur Baden-Württemberg (CSBW) und dem LfV ausgerichtete Format informiert Kandidaten und Kandidatinnen über Gefahren im digitalen und analogen Raum und gibt konkrete Handlungsempfehlungen für Schutzmaßnahmen, zum Beispiel im Zusammenhang mit Wahlkampfveranstaltungen. Über Maßnahmen, Angebote und Anlaufstellen von Polizei, CSBW und LfV im Zusammenhang mit der Wahl zum 21. Deutschen Bundestag wurde zentral auf der Homepage des Ministeriums des Inneren, für Digitalisierung und Kommunen Baden-Württemberg informiert, siehe hierzu etwa die Informationsmaterialien, welche unter *https://im.baden-wuerttemberg.de/de/land-kommunen/lebendige-demokratie/wahlen/sicherheit-im-wahlkampf* und *https://im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/sicherheit-im-wahlkampf* abrufbar sind.

Im Hinblick auf die Landtagswahl 2026 bleiben Cyberangriffe fremder Mächte denkbar. Auch die Agitation von Extremisten und extremistischer Gruppierungen im Kontext der Wahl analysiert das LfV und steht dazu im Austausch mit dem Bundesamt für Verfassungsschutz und den Landesbehörden. Im Bereich der Cybersicherheit bei der Landtagswahl 2026 ist das LfV immer dann zuständig, wenn sich Cyberspionage und Cybersabotage fremder Staaten gegen politische Stellen in Baden-Württemberg richten. Bereits jetzt ist geplant, die bereits zur Bundestagswahl 2025 implementierten Sensibilisierungsmaßnahmen der Cyberabwehr fortzuentwickeln und erneut anzubieten. Dazu gehört beispielsweise eine frühzeitige Durchführung von Präventionsmaßnahmen speziell für Abgeordnete bzw. Kandidatinnen und Kandidaten für die jeweiligen Wahlkreise sowie ein Monitoring möglicher Schwachstellen und die Erstellung von Sicherheitshinweisen.

Das LfV wird weiterhin sowohl anlassunabhängig als auch bei konkreten Verdachtsmomenten die an Wahlen beteiligten Behörden sowie politische und staatliche Stellen in Baden-Württemberg für die Gefahren im Zusammenhang mit der Landtagswahl sensibilisieren und als Ansprechpartner für Fragen zu einer möglichen Einflussnahme bei der Landtagswahl 2026 zur Verfügung stehen. Hierzu werden auch künftig Lagebilder verschickt, bei Bedarf Warnmeldungen gesteuert und potenziell betroffene Stellen individuell beraten.

Politische Wahlen entfalten erfahrungsgemäß bereits im Vorfeld des Wahltermins auch polizeiliche Relevanz. Mit Näherrücken eines Wahltags ist regelmäßig mit einer Intensivierung des öffentlichen Diskurses und daher auch mit einem erhöhten Aufkommen an Straftaten im Bereich der Politisch motivierten Kriminalität zu rechnen. Der Schutz von Wahlbewerberinnen und Wahlbewerbern sowie Wahlveranstaltungen hat dabei für die Polizei Baden-Württemberg höchste Bedeutung.

Im Vorfeld von Bundes- und Landtagswahlen wird durch das LKA BW eine Informationssammelstelle eingerichtet. Hier werden fortlaufend alle entsprechenden Erkenntnisse erhoben, zusammengeführt und bewertet. Zum Schutz von polizeilich bekannten Veranstaltungen in Zusammenhang mit Wahlen werden auf Grundlage einer polizeilichen Gefährdungsbewertung die lageorientiert erforderlichen polizeilichen Maßnahmen durch die regionalen Polizeipräsidien getroffen. Parteiveranstaltungen werden individuell betrachtet und die erforderlichen Maßnahmen lageangepasst durchgeführt.

Die Broschüre „Sicherheit für Amts- und Mandatsträgerinnen und -träger sowie andere Personen mit Gefährdungsrisiko“ der Polizei Baden-Württemberg enthält umfassende Verhaltensempfehlungen und zeigt vielfältige Handlungsoptionen auf. Sie soll Personen, die aufgrund ihrer Stellung im öffentlichen Leben einer höheren Gefährdung unterliegen, dazu anhalten, ihr Verhalten im Alltag zu reflektieren, mögliche Tatgelegenheiten zu identifizieren und für ein sicherheitsbewusstes Verhalten sensibilisieren.

Insbesondere während des Wahlkampfes können Politikerinnen und Politiker sowie ihre Parteien und Büros zunehmend zum Ziel von Angriffen werden. Die Polizei Baden-Württemberg gibt mit dem Leitfaden „Sicher im Wahlkampf“ hilfreiche Empfehlungen. So können mögliche Sicherheitslücken geschlossen und im Ernstfall richtig reagiert werden.

Zudem steht Amts- und Mandatsträgerinnen und -trägern mit der Zentralen Ansprechstelle für Amts- und Mandatsträger (ZAMAT) beim LKA BW über die Rufnummer 0711 5401-3003 ganzjährig und rund um die Uhr ein qualifiziertes Beratungsangebot zur Verfügung. Die im Juli 2019 auf Initiative des Innenministers Thomas Strobl eingerichtete Ansprechstelle bietet eine niederschwellig zugängliche Ersteinschätzung und -beratung durch staatsschutzerfahrene Kriminalbeamtinnen und -beamte und vermittelt lageorientiert an die spezialisierten Ansprechpersonen vor Ort bei den regionalen Polizeipräsidien. Seit November 2023 wird die ZAMAT um ein psychosoziales Beratungsangebot durch eine Psychologin ergänzt. Damit steht ein umfassendes Beratungsangebot zur Verfügung, welches neben den Aspekten der Gefahrenabwehr und Strafverfolgung auch psychosoziale Fragestellungen qualifiziert abdeckt.

Mit Blick auf die Gefahren im digitalen Raum, auch im Vorfeld oder während einer Wahl, steht die Zentrale Ansprechstelle Cybercrime (ZAC) des LKA BW bei IT-Sicherheitsvorfällen über die Rufnummer 0711 5401-2444 oder per E-Mail als kompetenter Ansprechpartner für Unternehmen sowie andere öffentliche und nicht-öffentliche Stellen zur Verfügung. Die ZAC kann bei einem konkreten Cybervorfall beratend unterstützen, zeitnah polizeiliche Erstmaßnahmen veranlassen und sich anlassbezogen eng mit der CSBW und dem LfV abstimmen.

Der CSBW obliegt – neben den vielfältigen Aufgaben zum Schutz der öffentlichen Stellen vor Cyberangriffen – auch der Schutz gesellschaftlich relevanter Prozesse im Cyberraum nach den Vorgaben des Cybersicherheitsgesetzes Baden-Württemberg. In diesem Kontext und auch als Erkenntnis aus den in der Beantwortung zur Kleinen Anfrage angesprochenen Einflussnahmen wurde anlässlich der Bundestagswahl die Landeswahlleitung sowohl im Vorfeld als auch am Wahltag selbst beraten und operativ unterstützt. So wurde beispielsweise ein gezielt auf Themen der Wahl abgestimmtes Cybermonitoring eingerichtet, um einschlägige Quellen auf Hinweise nach geplanten oder erfolgenden Angriffen oder Manipulationsversuchen zu durchsuchen. Darüber hinaus wurde die wahlunterstützende IT durch die CSBW auf Resilienz hin untersucht. Die potenziellen Gefährdungen durch Deepfakes und Bildmanipulationen werden von der CSBW nicht nur im Kontext von Wahlen aufgegriffen. Dazu hat die CSBW bereits im vergangenen Jahr ein Factsheet (abrufbar unter *https://www.cybersicherheit-bw.de/sites/default/files/2024-05/CSBW-Factsheet_barrierefrei_Deepfake.pdf*) sowie ein Erklärvideo (abrufbar unter *https://www.cybersicherheit-bw.de/erklaervideos-zur-cybersicherheit*) bereitgestellt. Künftig wird diese Thematik auch im Schulungsangebot der CSBW Niederschlag finden und damit auch den mit Wahlen befassten Mitarbeiterinnen und Mitarbeitern in den Kommunen zugänglich gemacht. Die dargelegten Maßnahmen, Unterstützungsleistungen und Informationsangebote der CSBW werden auch bei der anstehenden Landtagswahl 2026 in Baden-Württemberg zur Verfügung gestellt.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen