Mecklenburg-Vorpommern
Ministerium für Inneres
und Bau

Informationsbroschüre des Verfassungsschutzes

Mecklenburg-Vorpommern

für
Parteien und Kandidierende
anlässlich der
Landtagswahl 2026 in MV

Hybride Bedrohungen

Die Landtagswahl 2026 in Mecklenburg-Vorpommern findet in Zeiten hybrider Bedrohungen statt. Hierbei handelt es sich um Aktivitäten fremder Staaten, mit denen das Sicherheitsgefühl der Bevölkerung und die politische Stabilität erschüttert werden sollen. Eine zentrale Bedeutung kommt dabei Wahlen als demokratischen Entscheidungszeitpunkten zu. Mit dieser Informationsbroschüre möchte daher der Verfassungsschutz vor allem Parteien und Kandidierende über potentielle Gefahren sowie Sicherheitshinweise informieren.

Stand: Juni 2026

1. Grundlagen und Gefährdungslage

Der Begriff „hybride Bedrohungen“ beschreibt Strategien, bei denen durch fremde Staaten unterschiedliche Mittel kombiniert werden, um Staat, Bevölkerung und Wirtschaft ohne offene Konfrontation zu beeinflussen oder zu destabilisieren.

Hybride Bedrohungen: eine Kombination verschiedener Mittel

„Hybrid“ bedeutet in diesem Zusammenhang: Es werden verschiedene Instrumente gleichzeitig oder abgestimmt eingesetzt.

Dazu können unter anderem gehören:

- ➜ gezielte Desinformation, d. h. manipulativ verkürzte oder verfälschte Darstellungen
- ➜ Einflussversuche auf öffentliche Debatten
- ➜ Cyberangriffe auf IT-Systeme
- ➜ Versuche, Vertrauen in staatliche Institutionen zu untergraben
- ➜ Spionage und Sabotage

Hybride Bedrohungen werden in der sicherheitspolitischen Debatte zunehmend als komplexes Phänomen verstanden: Sie verbinden klassische nachrichtendienstliche und außenpolitische Methoden und Einflussnahmeversuche fremder Mächte mit illegitimen Mitteln wie Desinformation sowie mit modernen Angriffsmustern wie Cyberangriffen, Sabotage und dem Einsatz von sogenannten Low-Level-Agents.

Welche Gefährdungslage zeigt sich aktuell?

Das Bundesinnenministerium berichtet, dass Deutschland seit Beginn des russischen Angriffskrieges gegen die Ukraine einer erhöhten Gefährdungslage gegenübersteht und hybride Bedrohungen ein Schwerpunkt der nationalen Sicherheitspolitik sind. Dazu zählen Cyberangriffe, gezielte Desinformation sowie weitere Formen der Beeinflussung. Bei der Bundestagswahl 2025 wurden zahlreiche Einflussnahmen registriert, hauptsächlich mit russischer Verantwortung.

Das Bundesamt für Verfassungsschutz weist darauf hin, dass russische Spionage, Sabotage und Desinformation in den letzten Jahren deutlich zugenommen haben und Teil eines umfassenden Vorgehens sind, gesellschaftliche Strukturen zu beobachten und zu beeinflussen.

2. Typische Angriffsmuster und Risiken hybrider Bedrohungen

Cyberangriffe Diese können IT-Systeme kompromittieren, Daten ausspähen oder Abläufe stören.	**Spionage** Fremde Nachrichtendienste verfolgen weiterhin Spionageaktivitäten, um sensible Informationen zu erlangen. Dabei spielen digitale Kanäle, verdeckte Netzwerke, Social-Engineering und Low-Level-Agents eine Rolle.
Sabotage Sabotagehandlungen können physische oder digitale Störungen auslösen und somit große Bevölkerungsteile betreffen. Begleitende Propaganda oder Desinformation kann diese Effekte verstärken, etwa indem sie in der Öffentlichkeit Unsicherheit schürt.	**Desinformation** Gezielte Falschinformationen, unvollständige oder manipulierte Inhalte sollen die Bevölkerung verunsichern, polarisieren und das Vertrauen in den Staat auf Dauer zerstören.

Die EU-Einrichtung EUvsDiSinfo hat in den vergangenen Jahren bereits fast 20.000 Fälle von Desinformation aus dem internationalen Informationsraum identifiziert und entlarvt.[1]

Parteien und Kandidierende sollten folgende mögliche Angriffe berücksichtigen:

- ➜ Phishing-Mails + Messenger und kompromittierte Accounts
- ➜ Gezielte Desinformation über soziale Netzwerke
- ➜ Fake-Webseiten (gefälschte Nachrichtenquellen) oder gefälschte Wahlkampfinhalte
- ➜ Deepfakes von Kandidierenden oder Parteivertretern insb. KI-generierte Video- und Audio-Deepfakes
- ➜ KI-generierte Fake-Anrufe bei Wählern zur Wählerabschreckung (Robo-Calls)
- ➜ Manipulation öffentlicher Debatten durch Bots und Trollnetzwerke
- ➜ Cyberangriffe auf IT-Systeme, Cloud-Dienste und Webseiten
- ➜ Datendiebstahl und Veröffentlichung interner Informationen

Hieraus ergeben sich folgende Risiken für Parteien und Kandidierende:

- ➜ Verlust sensibler Kommunikationsdaten
- ➜ Beschädigung der öffentlichen Glaubwürdigkeit
- ➜ Beeinflussung von Wählerinnen und Wählern
- ➜ Störung von Wahlkampfveranstaltungen oder digitalen Kanälen
- ➜ Reputationsschäden durch gefälschte Inhalte
- ➜ Rechtliche und organisatorische Folgen nach Sicherheitsvorfällen

[1] https://euvsdisinfo.eu/de/ *(Stand: 08.06.2026, 14:08 Uhr)*

3. Schutzmaßnahmen

Angesichts der dargestellten Sicherheitsrisiken werden die nachfolgenden Schutzmaßnahmen empfohlen.

3.1. Präventive IT-Sicherheit

- ✓ Mehrfaktor-Authentifizierung für alle Accounts aktivieren
- ✓ Starke und einzigartige Passwörter verwenden („Passwortmanager")
- ✓ Regelmäßige Schulungen für Mitarbeitende und Ehrenamtliche durchführen (Phishing, Social Engineering)
- ✓ Software, Betriebssysteme und Plugins aktuell halten
- ✓ Verdächtige E-Mail-Dateianhänge oder Links niemals ungeprüft öffnen
- ✓ Sensible Kommunikation verschlüsseln
- ✓ Backups regelmäßig erstellen und testen
- ✓ Zugriffsrechte auf notwendige Personen beschränken

3.2. Vorbereitung auf Cyber-Angriffe

- ✓ Verantwortliche Personen und Eskalationswege festlegen
- ✓ Kontakt zu IT-Sicherheitsdienstleistern vorbereiten
- ✓ Festlegen, welche Systeme „überlebensnotwendig" sind und daher zuerst wieder funktionieren müssen

3.3. Vorbereitung auf Desinformation

- ✓ Krisenteam organisieren: Wer entscheidet im Ereignisfall über die Reaktion? Wie sind die Erreichbarkeiten?
- ✓ Monitoring festlegen: Tools, z. B. Google Alerts oder Talkwalker Alerts, helfen beim Erkennen von Auffälligkeiten (z. B. Kandidierendenname in Verbindung mit negativen Schlüsselwörtern) und benachrichtigen automatisch
- ✓ Verifizierte Accounts stärken: Durch die die Einrichtung von offiziellen Accounts können Bürgerinnen und Bürger einfacher das Original erkennen
- ✓ Website vorbereiten: Auf der Webseite kann ein inaktiver Bereich eingerichtet werden, der bei Desinformation zügig mit einer Richtigstellung öffentlich gemacht werden kann

3.4. Reaktion bei Desinformation

- ✓ Ruhe bewahren
- ✓ Echtheit: Ist das Material echt, kontextlos oder KI-generiert?
- ✓ Bilder: Sind Hände, Ohren, Hintergründe und Texte fehlerbehaftet?
- ✓ Audios: Ist die Betonung unnatürlich und fehlen Atemzüge?
- ✓ Videos: Natürliche Lippen- und Wimpernbewegungen?
- ✓ Quelle: Hat ein anonymer Bot oder eine reale Person zuerst gepostet?
- ✓ Rückwärtssuche: Ursprung eines Bildes mit Google Bildersuche oder TinEye prüfen
- ✓ Risiko einschätzen
- ✓ **Szenario 1:** Die Desinformation hat geringe Reichweite -> strategische Zurückhaltung, um ungewollt verstärkte Verbreitung zu vermeiden
- ✓ **Szenario 2:** Die Desinformation geht viral -> Sofortige Reaktion
- ✓ Bei Reaktion niemals die Falschbehauptung als Einstieg nutzen
- ✓ Mit der Wahrheit bzw. Fakten starten
- ✓ Desinformation als solche benennen und davor warnen (ohne Verlinkung)
- ✓ Wahrheit und Kontext wiederholen
- ✓ Screenshot der Desinformation mit dickem roten Stempel „FAKE“ oder „KI-GENERIERT“ posten, damit Dementi nicht als Verbreitung missverstanden wird
- ✓ Melde-Funktionen der Social-Media-Plattformen nutzen: „Wahlmanipulation“ oder „Impersonation“
- ✓ Vertrauenswürdige Journalistinnen und Journalisten einbeziehen und Fälschungsbeweise zeigen
- ✓ Unterstützungsteam sollte Dementi bzw. Faktencheck teilen und nicht in Kommentaren des Fakes argumentieren
- ✓ Artikel, Bilder usw. zügig speichern, zumindest als Screenshot
- ✓ Strafanzeige erstatten
- ✓ Auswertung der Reaktion und „lessons learned“

4. Schutzmaßnahmen des Landes MV

Mit hybriden Bedrohungen geht das Land MV besonnen und strukturiert um. Im Folgenden möchten wir Ihnen einen Überblick über die Schutz- und Unterstützungsmaßnahmen des Landes geben.

Strukturelle Resilienz im Land Mecklenburg-Vorpommern

Hybride Bedrohungen sind keine Einzelphänomene, sondern Teil einer komplexen sicherheitspolitischen Lage im gesamtdeutschem und sogar europäischen Raum. Dementsprechend erfolgen Prävention und Reaktion strukturiert und abgestimmt im ganzen Bundesgebiet.

Das Land Mecklenburg-Vorpommern verfügt über etablierte Schutzmechanismen, die kontinuierlich weiterentwickelt werden. Ziel ist es, staatliche Handlungsfähigkeit, Informationssicherheit und Vertrauen in öffentliche Institutionen zu sichern.

Lagebewertung, Monitoring und Anpassung der Sicherheitsarchitektur

Hybride Bedrohungen werden fortlaufend analysiert. Dazu gehören:

- Beobachtung sicherheitsrelevanter Entwicklungen
- Bewertung von Desinformationsmustern
- Austausch mit Bundesbehörden und anderen Ländern
- Einbindung fachlicher Expertise

Im Ergebnis werden Konsequenzen für die Sicherheitsarchitektur des Landes gezogen und Anpassungen umgesetzt.

Die Landesregierung hat den Verfassungsschutz MV als Single Point of Contact (SPOC) des Landes MV für Angelegenheiten der hybriden Bedrohungen in der Bundesrepublik Deutschland benannt. Der Verfassungsschutz MV – als Abteilung des Innenministeriums MV – sorgt für eine enge Zusammenarbeit mit anderen Ländern und den Bundesbehörden.

Darüber hinaus organisiert der Verfassungsschutz MV das „MV Forum Hybrid“. Hierbei handelt es sich um eine ressortübergreifende Plattform des Landes MV, in der Informationen zu hybriden Bedrohungen ausgetauscht und Maßnahmen abgestimmt werden. Jedes Ressort verfügt über einen eigenen ressorteigenen Ansprechpartner als Bindeglied zum SPOC für das Themenfeld hybride Bedrohungen.

IT-Sicherheitsstrukturen

Hybride Bedrohungen zeigen sich oftmals in Gestalt von Cyberangriffen. Die Informationssicherheit in der Landesverwaltung basiert auf klar definierten organisatorischen und technischen Maßnahmen, unter anderem:

- Zentrale und dezentrale IT-Sicherheitsstrukturen
- Monitoring von Netzwerken und Systemen
- Notfall- und Wiederanlaufpläne einschließlich CERT M-V

Krisen- und Notfallstrukturen

Für außergewöhnliche Ereignisse wurden Krisen- und Notfallmechanismen entwickelt, die aktiviert werden können.

Dazu zählen:

- Krisenstäbe
- Notfallpläne
- abgestimmte Melde- und Entscheidungswege

Resilienz entsteht gemeinsam

Hybride Bedrohungen betreffen die gesamte Gesellschaft, insbesondere die Bevölkerung, Behörden und Unternehmen. Durch Aufmerksamkeit, Sensibilität für Manipulationsversuche, IT-Sicherheitsmaßnahmen und Notfallvorsorge kann jede Person einen Beitrag zu einer resilienten, d. h. widerstandsfähigen Gesellschaft leisten.

Weitere nützliche Informationen zu hybriden Bedrohungen sowie staatlichen und privaten Schutzmaßnahmen:

- Bundesinnenministerium „Sensibilisierung im Umgang mit hybriden Bedrohungen einschließlich Desinformation“: BMI - Publikationen - Sensibilisierung im Umgang mit hybriden Bedrohungen einschließlich Desinformation (BLoAG)
- Bundesinnenministerium „FAQ Desinformation im Kontext des russischen Angriffskrieges gegen die Ukraine“: BMI - Homepage - FAQ - Desinformation im Kontext des russischen Angriffskrieges gegen die Ukraine
- Informationen des Bundesamts für Verfassungsschutz: Bundesamt für Verfassungsschutz - Homepage - Hybride Angriffe - Viele Nadelstiche gegen die Demokratie
- Informationen der EU zu Desinformation mit umfangreicher Datenbank von Desinformationsaktivitäten: www.euvsdisinfo.eu
- Videos, Tipps, Beispiele u.v.m. der Bayern-Allianz gegen Desinformation: Infoportal Gelogen?!
- Für junge Menschen und Lehrerinnen und Lehrer bieten die Deutsche Presse Agentur und die Hamburger Behörde für Kultur und Medien mit weiteren Partnern Erklärvideos, Online-Spiele, Workshops und eine Datenbank u. a. zu Fake News, Verschwörungstheorien und Quellenchecker: www.usethenews.de
- Das Bundesamt für Sicherheit in der Informationstechnik bietet umfangreiche Informationen für Bürger, Unternehmen und Behörden zu Aspekten der IT-Sicherheit: www.bsi.bund.de
- Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe bietet umfangreiche Verhaltenstipps zu Notfallvorsorge und Selbstschutz für Bürgerinnen und Bürger und Behörden: www.bbk.bund.de
- Eine Broschüre des BBK für Bürgerinnen und Bürger informiert über private Notfallvorsorge und Selbstschutz: Ratgeber: Vorsorgen für Krisen und Katastrophen - BBK
- Informationen des Verfassungsschutzes MV zu Spionageabwehr und Wirtschaftsschutz: Spionageabwehr und Wirtschaftsschutz

Ansprechpartner

Allgemeine Fragen zu hybriden Bedrohungen
Verfassungsschutz Mecklenburg-Vorpommern
SPOC Hybride Bedrohungen
E-Mail: spoc_hybrid@im.mv-regierung.de
Telefon: 0385/7420-0
www.verfassungsschutz-mv.de

Zentrale Meldestelle (SPOC) für IT-Sicherheitsvorfälle
Computer Emergency Response Team (CERT M-V)
Telefon: +49 385 588 11333
E-Mail: cert@mv-regierung.de

Bei akuter Gefahr
Polizei – Notruf 110