Mecklenburg-Vorpommern
Ministerium für Inneres
und Bau

35 Jahre Verfassungsschutz Mecklenburg-Vorpommern

Informationsbroschüre des Verfassungsschutzes

Mecklenburg-Vorpommern

für
Bürgerinnen und Bürger
zum Thema

Hybride Bedrohungen

Hybride Bedrohungen sind zu einer erheblichen Gefährdung für die Sicherheit Deutschlands und Mecklenburg-Vorpommerns geworden. Hierbei handelt es sich um gezielte Aktivitäten fremder Mächte, mit denen das Sicherheitsgefühl der Bevölkerung und das Vertrauen in staatliche Institutionen erschüttert werden sollen. Mit dieser Broschüre möchte der Verfassungsschutz über potentielle Gefahren informieren, Sicherheitshinweise geben und damit einen Beitrag zur Stärkung der gesellschaftlichen Resilienz gegenüber hybriden Bedrohungen leisten. Im Mittelpunkt steht die Gefährdung durch gezielte Desinformation fremder Mächte.

Stand: Juni 2026

1. Grundlagen und Gefährdungslage

Der Begriff „hybride Bedrohungen“ beschreibt Strategien, bei denen durch fremde Staaten unterschiedliche Angriffsmittel 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 kombiniert und/oder abgestimmt eingesetzt.

Dazu können unter anderem gehören:

- ➜ gezielte Desinformation, d. h. die Verbreitung von falschen oder unvollständigen bzw. irreführenden Informationen
- ➜ Einflussnahmeversuche 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 gezielter Desinformation sowie mit modernen Angriffsmustern wie Cyberattacken, Sabotage und dem Einsatz von sogenannten Low-Level-Agents („Wegwerf-Agenten“).

Was sind hybride Bedrohungen?

Nach dem Bundesinnenministerium (BMI) gehören zur Kategorie der hybriden Bedrohungen nicht nur Desinformation, sondern auch Aktivitäten wie Cyberangriffe, Spionage und Sabotage. Dazu zählen Aktionen, die:

- ➜ staatliche Abläufe stören,
- ➜ digitale oder physische Infrastrukturen angreifen,
- ➜ vertrauliche Informationen ausspähen,
- ➜ und Manipulationsversuche durchführen, die Vertrauen in staatliche Abläufe untergraben.

Welche Gefährdungslage zeigt sich aktuell?

Das Bundesamt für Verfassungsschutz (BfV) betont, dass Spionage, Sabotage und gezielte Desinformation seit dem Beginn des russischen Angriffskrieges auf die Ukraine 2022 in Deutschland stark zugenommen haben und Teil eines umfassenden Vorgehens sind, gesellschaftliche Strukturen zu beobachten und zu beeinflussen.

Ziel ist häufig nicht ein einzelnes Schadensereignis, sondern die schrittweise Verunsicherung und Schwächung staatlicher Strukturen und der Gesellschaft.

Das BMI berichtet, dass Deutschland seit Beginn des Krieges gegen die Ukraine einer erhöhten Sicherheitslage gegenübersteht und hybride Bedrohungen ein Schwerpunkt der nationalen Sicherheitspolitik sind. Dazu zählen Cyberangriffe, gezielte Desinformation sowie weitere Formen der Beeinflussung.

2. Typische Angriffsmuster – kurz erklärt

Cyberangriffe Diese können IT-Systeme kompromittieren, Daten ausspähen oder Abläufe stören. Solche Aktivitäten richten sich u. a. gegen Behörden, kritische Infrastrukturen und Unternehmen.	**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. Begleitende Propaganda oder Desinformation kann diese Effekte verstärken, etwa indem sie in der Öffentlichkeit Unsicherheit schürt. Insbesondere hier wird vermehrt auf Low-Level-Agents gesetzt.	**Desinformation** Gezielte Falschinformationen oder manipulierte Inhalte können das Vertrauen in Behördenprozesse untergraben. Das BMI stuft Desinformation als Teil der hybriden Bedrohungslandschaft ein, insbesondere wenn sie mit staatlichen Akteuren in Verbindung gebracht werden kann.

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

Weitere nützliche Informationen zur Gefährdungslage hybrider Bedrohungen

- ➜ Informationen des Bundesamts für Verfassungsschutz: https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefaehrdung-russische-spionage-sabotage-desinformation.html
- ➜ Informationen des Bundesinnenministeriums: https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefaehrdung-russische-spionage-sabotage-desinformation.html
- ➜ Informationen der EU zu Desinformation mit umfangreicher Datenbank von Desinformationsaktivitäten: www.euvsdisinfo.eu

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

3. Erkennen und Einordnen von Desinformation

Hybride Bedrohungen laufen häufig nicht offen, sondern eher subtil ab. Übergeordnetes Ziel fremder Mächte beim Einsatz hybrider Mittel ist es, Unsicherheit zu erzeugen, Abläufe zu stören oder Vertrauen zu beeinträchtigen um Deutschland nachhaltig zu destabilisieren. Diese Form der Destabilisierung wirkt auf alle gesellschaftlichen Ebenen ein, von der Politik über die Verwaltung und von der Wirtschaft bis in die einzelnen Haushalte. Ein sehr großflächig wirkendes Mittel ist der illegitime Einflussnahmeversuch durch gezielte Desinformation.

Illegitim, weil die Herkunft der falschen Information verschleiert oder ahnungslosen Urhebern beispielsweise Parteien, Personen des öffentlichen Lebens oder Leitmedien zugeschrieben wird. Die Inhalte sind in der Regel geprägt von:

- ⚠ starker Emotionalisierung
- ⚠ fehlenden Quellen
- ⚠ künstlicher Empörung
- ⚠ vereinfachten Schuldzuweisungen

Auch zunächst seriös wirkende Inhalte können manipuliert, aus dem Zusammenhang gerissen oder künstlich verstärkt worden sein.

> Manipulative Inhalte sollen häufig nicht informieren, sondern Angst, Wut oder Unsicherheit verstärken. Hierzu werden falsche oder unvollständige bzw. irreführende Informationen bewusst gestreut.

Weitere nützliche Informationen zum Erkennen von hybriden Bedrohungen insbesondere Desinformation finden Sie hier:

- ➜ Videos, Tipps, Beispiele u.v.m. der Bayern-Allianz gegen Desinformation: https://lass-dich-nicht-manipulieren.bayern.de/de?category
- ➜ Informationen der EU zu Desinformation mit umfangreicher Datenbank von Desinformationsaktivitäten: www.euvsdisinfo.eu
- ➜ 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
- ➜ Informationen der Bundesregierung: https://www.bundesregierung.de/breg-de/aktuelles/was-ist-desinformation-1875148
- ➜ Artikel der Stiftung Wissenschaft und Politik: https://www.swp-berlin.org/10.18449/2024A69/

4. Richtig handeln gegen Desinformation und für private Sicherheit

Die 5 wichtigsten Verhaltenshinweise gegen Desinformation

✓ **Quellen prüfen**
Woher stammt die Information?

✓ **Nicht sofort teilen**
Emotionale Inhalte bewusst hinterfragen.

✓ **Mehrere Medien vergleichen**
Berichten andere seriöse Quellen ebenfalls darüber?

✓ **Bilder und Videos kritisch betrachten**
KI kann täuschend echte Inhalte erzeugen.

✓ **Ruhe bewahren**
Manipulation wirkt besonders stark bei Stress, Angst und Unsicherheit.

Darüber hinaus gilt:

✓ IT-Sicherheit ernst nehmen und die offiziellen Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) beachten

✓ Vorsorge ist besser als Nachsorge: Private Notfall- und Krisenvorsorge hilft sich und seine Mitmenschen in einer Gefahrensituation schützen zu können

Ihre Aufmerksamkeit macht den Unterschied: Eine informierte und besonnene Gesellschaft ist widerstandsfähiger gegen Manipulation und Verunsicherung.

Weitere nützliche Informationen zum richtigen Verhalten bei hybriden Bedrohungen

➜ 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: https://www.bbk.bund.de/DE/Warnung-Vorsorge/Vorsorge/Ratgeber-Checkliste/ratgeber-checkliste_node.html

5. 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

Schutz demokratischer Verfahren

Insbesondere in sensiblen Phasen – etwa bei der Landtagswahl 2026 – werden zusätzliche Schutzmechanismen aktiviert.

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 zum Verfassungsschutz Mecklenburg-Vorpommern
Verfassungsschutz MV
E-Mail: info@verfassungsschutz-mv.de
Telefon: 0385/7420-0
www.verfassungsschutz-mv.de

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

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