CeMAS

Policy Brief

Umgang mit Desinformation und Informationsmanipulation bei den EU-Wahlen 2024

Handlungsempfehlungen

Im Kontext der Wahl zum Europäischen Parlament im Juni 2024 ist mit einem Anstieg illegitimer Einflussversuche zu rechnen. Darauf bezogene Schutz- und Eindämmungsbemühungen sollten daher umfassend und wirksam gestaltet sein. Sie müssen frühzeitig und langfristig ansetzen und die Komplexität und zyklische Wiederholung des Problems im Blick haben. Wir empfehlen folgende Maßnahmen:

1

Mit transparenter Kommunikation Wissen und Vertrauen fördern

Die transparente und umfassende Kommunikation verlässlicher Information kann den Wissensstand der Bürger:innen sowie ihr Vertrauen gegenüber demokratischen Institutionen stärken, bevor Falsch- und Desinformation diese angreifen. Wer irreführende Behauptungen gesehen hat, kann diese anhand des Informationsangebots prüfen. Eine solche Kommunikation sollte von all jenen Institutionen und Organisationen geleistet werden, die typischerweise von Falsch- und Desinformation im Kontext von Wahlen adressiert werden. Die Umsetzung variiert entlang der Rolle: Die Bundeswahlleiterin etwa schafft Klarheit über den Wahlprozess sowie getroffene Schutzmaßnahmen, während Ministerien umfassend über ihre Arbeit und Ziele informieren.

2

Zusammenarbeit stärken, um Spaltungsversuchen entgegenzutreten

Spaltungsversuchen sollte durch Zusammenarbeit und Demonstration von Zusammenhalt begegnet werden. Konkret sollten sich all jene Akteur:innen vernetzen und in einen regelmäßigen Austausch treten, die sich dem Schutz vor und der Abwehr von illegitimer Einflussnahme widmen. So lassen sich eigene Werte schützen und die kollektive Resilienz und Wehrhaftigkeit fördern. Frühzeitige Information über aktuelle Angriffe etwa kann andere befähigen, diese wirksam abzuwehren. Stärken und Ressourcen einer Vernetzungspartnerin können Defizite eines anderen Partners ausgleichen und so die kollektive Wehrhaftigkeit stärken.

3

Adressieren der vollständigen Bandbreite illegitimer Einflussversuche auf Wahlen

Konkrete Bemühungen zum Schutz von Wahlen vor illegitimen Einflussversuchen sollten deren Bandbreite in den Blick nehmen. Typische Ziele sind das Zersetzen von Vertrauen in die Demokratie, das Diskreditieren von Parteien und Kandidat:innen sowie das Abschrecken von Wähler:innen vom Wahlgang. Um diese Ziele zu erreichen können digitale (z. B. Cyberangriffe), physische (z.B. Drohungen gegenüber Wahlhelfer:innen) oder kommunikative Mittel (z. B. Desinformation) eingesetzt werden. Als mögliche Verbreitungskanäle sollten neben sozialen Medien auch weitere digitale sowie analoge Formate beachtet werden, wie die gefälschten Webseiten der russischen Doppelgängerkampagne sowie die irreführenden Flyer zur Corona-Schutzimpfung der Freiheitsboten deutlich gezeigt haben.

4 Solide Gestaltung der Maßnahmen durch Evidenz, Frameworks und Best Practice

Schutz- und Eindämmungsmaßnahmen sollten sich an aktueller wissenschaftlicher Evidenz orientieren sowie auf bestehenden Frameworks, Leitfäden und bewährten Praktiken aufbauen. Die OECD-Empfehlungen zur Kommunikation im Umgang mit Desinformation helfen, Angriffsflächen zu verringern. Das ABCDE-Framework kann zur strukturierten Ersterfassung von Vorfällen genutzt werden. Orientierung für reaktive Maßnahmen bietet das Reaktionsframework des EAD. Die standardisierte Erfassung im STIX-Format stellt Vergleichbarkeit her und ermöglicht den Austausch mit Vernetzungspartner:innen.

5 Verringern der Angriffsfläche durch Identifikation von Zielen und Risiken

Die Risiken für eigene Ziele und Prioritäten sollten im Vorfeld identifiziert werden. Dazu gehört auch Cybersecurity, sowie das Einbeziehen erweiterter Bereiche von Staat und Gesellschaft, die von Angriffen betroffen sein können (z. B. Ministerien oder Kommunalebene). Erhebungen zur Stimmung der Bevölkerung können hilfreichen Kontext liefern. So kann die Angriffsfläche durch frühzeitige Identifikation und Umsetzung des Anpassungsbedarfs verringert werden. Eigene Ziele und Risiken sowie Erfahrungswerte aus früheren Vorfällen (z. B. Fall Lisa) sollten in ein systematisches Debatten-Monitoring integriert werden, um risikoreiche Entwicklungen schnell zu identifizieren und eindämmen zu können.

6 Wirksame Schutzbemühungen brauchen Ressourcen und gute Organisation

Es bedarf der langfristigen Bereitstellung ausreichender finanzieller, personeller, zeitlicher und kompetenztechnischer Ressourcen. Da sich Angriffsmodi und Risiken verändern können, muss außerdem sichergestellt sein, dass auch kurzfristig identifizierte Bedarfe zeitnah adressiert und bearbeitet werden können. Hierzu bedarf es ebenfalls klar definierter Rollen, Prozesse, Verantwortlichkeiten und Befugnisse.

7 Reaktive Gegenmaßnahmen koordiniert und fallbezogen angehen

Neben eigenen Reaktionsmöglichkeiten sollte angesichts akuter Fälle der Austausch mit Vernetzungspartner:innen genutzt werden, um die Bandbreite und Wirksamkeit der Schutzmaßnahmen zu steigern und akute Vorfälle einzudämmen. Mögliche Gegenmaßnahmen umfassen etwa das Aufdecken manipulativer Netzwerke, die Sanktionierung verantwortlicher Staaten oder die fundierte Kommunikation belastbarer Fakten zu einem Sachverhalt. Unter Einsatz der bereits genannten Methoden und Frameworks sollten Vorfälle analysiert und fallbezogen wirksame Maßnahmenkombinationen abgeleitet werden.

8 Einflussversuche auf Wahlen nachhaltig betrachten

Nach jedem Wahlzyklus sollten Erkenntnisse ausgewertet und in einen kontinuierlichen Verbesserungsprozess integriert, sowie Vernetzungspartner:innen zur Verfügung gestellt werden. Die Umsetzung und Wirksamkeit der Maßnahmen müssen regelmäßig überprüft und nachjustiert werden, um Nachhaltigkeit sicherzustellen. Illegitime Einflussversuche müssen als konstante, wandlungsfähige Bedrohung für demokratische Gesellschaften verstanden werden. Für Wahlen bedeutet das die Notwendigkeit einer frühzeitigen Antizipation und Vorbereitung, sowie konsequent abgeleitete und umgesetzte Schutz- und Gegenmaßnahmen, deren Gestaltung sich analog zu den Angriffsvektoren konstant weiterentwickelt. Erkenntnisse aus der EU-Wahl sollten so etwa zum Schutz der anstehenden Landtagswahlen 2024 oder der Bundestagswahl 2025 genutzt werden.

Redaktion:
Lea Frühwirth

Kontakt:
info@cemas.io

04. April 2024

Angaben gemäß § 5 TMG
CeMAS – Center für Monitoring,
Analyse und Strategie gGmbH
Konstanzer Straße 15A, D-10707 Berlin

CeMAS, das Center für Monitoring, Analyse & Strategie, bündelt interdisziplinäre Expertise zu Verschwörungsideologien, Desinformation, Antisemitismus & Rechtsextremismus.

Handelsregister: HRB 226823 B
Registergericht: Berlin
USt-ID-Nummer: DE 340877977

Vertreten durch:
Pia Lamberty und Josef Holnburger

Redaktionell verantwortlich:
Pia Lamberty und Josef Holnburger

Gefördert durch:
ALFRED LANDECKER FOUNDATION