

Fraktion DIE LINKE.Volt
Postfach Rathausplatz 1, 59423 Unna
Herrn Bürgermeister
Dirk Wigant
Kreisstadt Unna

Kreisstadt Unna, 16.01.2026

Antrag zur Initiierung und Einrichtung eines digitalen Aufmerksamkeits- und Resilienz-Programms (DARP) der Stadt Unna

Sehr geehrter Herr Bürgermeister Wigant,

Die Fraktion DIE LINKE.Volt stellt für die Ratssitzung am 05.02.2026 folgenden Antrag:

Beschlussvorschlag:

1.

Der Rat der Stadt Unna beauftragt die Verwaltung Veranstaltungen vorzuplanen, vorzubereiten und durchzuführen. Den bereits bestehenden Institutionen kommt hierbei eine besondere Bedeutung zu. Hierbei liegt der Schwerpunkt auf der Initiierung eines gesamtheitlichen Netzwerkes mit allen beteiligten Akteuren und einer Weiterentwicklung bereits bestehender Formate unter Berücksichtigung der aktuellen gesamtgesellschaftlichen Entwicklungen.

2.

Der Rat der Stadt Unna beauftragt die Verwaltung eine Projektskizze mit Umsetzungsplan zur Institutionalisierung und Etablierung eines DARP (Steuerung/Koordinierung – Operative Umsetzung – Formate) zu erarbeiten und im 2. Quartal 2026 in einem Vorschlag zur Umsetzung an die zuständigen Gremien vorzulegen.

3.

Der Rat der Stadt Unna beauftragt die Verwaltung hierzu im Haushalt 2026 zunächst 5.000 Euro bereit zu stellen. Zudem soll durch die bereitgestellten Haushaltsmittel der Einsatz von Förderprogrammen geprüft werden.

4.

Die Stadt Unna berichtet anlassbezogen über den Fortschritt der Planungen und den Einsatz der Haushaltsmittel, spätestens jedoch zum Ende eines jeden Quartals in 2026.

Begründung:

I. Problembeschreibung:

1. Desinformation

Seit kurzem ist offiziell bekannt, dass Russland im Rahmen seiner **hybriden** Kriegsführung gegen Europa und Deutschland unter anderem massiven Einfluss auf unsere freien und unabhängigen Wahlen genommen hat. Dies geschieht mittels umfangreichen Desinformationskampagnen in sozialen Netzwerken, durch pro-russische Influencer und Rechtsextremisten. Zudem wurden Cyberangriffe auf die bundesdeutsche Flugsicherung nachgewiesen. Das Ziel von russischer Desinformation ist es, die deutsche Gesellschaft zu spalten und das Vertrauen in den Staat und seinen Institutionen zu schwächen.

<https://www.tagesschau.de/inland/botschafter-russland-cyberangriffe-100.html>

Durch die zunehmende Durchdringung von **künstlicher Intelligenz (KI)** und KI-Tools in digitalen Formaten sowie in sozialen Medien und Videoplattformen können Bilder und Videos, die mit KI erstellt wurden kaum noch von realen unterschieden werden (Deepfakes).

<https://www.fragzebra.de/antwort/kann-ki-unsere-demokratie-gef%C3%A4hrden>

Dies führt zwangsweise zu einer schnelleren Verbreitung von solchen Bildern und Videos. Dabei werden auch **Falschinformationen** verarbeitet und finden so einen weiteren Weg einer schnelleren Verbreitung. Dabei sieht sich nicht nur die gesamte Bevölkerung einer wachsenden Verbreitung von Falschinformationen ausgesetzt, sondern insbesondere vulnerable

Fraktion DIE LINKE.Volt
Im Stadtrat der Kreisstadt Unna
Postfach Rathausplatz 1, 59423 Unna

Vertreten durch:
Frau Hestia van Roest (Vorsitzende)
Herrn Thomas Franta (Vorsitzender)

Mail: Fraktion@dielinkevolt-unna.de
www.dielinkevolt-unna.de

Bevölkerungsgruppen, die zum Teil ungefiltert auf solche Informationen treffen. Hierbei können Kinder und Senioren genannt werden, die gerade in die digitale Medienwelt einsteigen, als auch Jugendliche, die digitale Medien bereits länger konsumieren. Dabei sind Jugendliche besonders empfänglich für Extreme und **Hassrede**, was zu Kriminalität und Radikalisierung führen kann.

<https://www.medienanstalt-nrw.de/hass.html>

2. Sabotage

Sabotage von **kritischer Infrastruktur** soll die Verletzlichkeit unseres Staates aufzeigen und wird ebenfalls dazu eingesetzt das Vertrauen in den Staat und seiner Institutionen zu schwächen. Meist soll das gesellschaftliche Zusammenleben erheblich gestört werden und damit Ängste, Vertrauensverlust und die öffentliche Meinung beeinflussen. Sabotage wird häufig vorbereitet und gezielt durchgeführt. Sabotage kann sowohl analog als auch digital durchgeführt werden und ist Teil eines hybriden Bedrohungsszenarios.

<https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/die-neue-bedrohung-sabotage-durch-fremde-nachrichtendienste.html#doc2095168bodyText3>

3. Cyberkriminalität

Die Zahl von **Cyberangriffen** auf **Bürgerinnen und Bürger** sowie auf die europäische und deutsche Wirtschaft und staatliche Einrichtungen nimmt massiv zu. Cyberangriffe mit dem Ziel das private und wirtschaftliche Vermögen sowie die Handlungsfähigkeit von staatlichen Institutionen zu schwächen haben auf mehreren Ebenen negative Auswirkungen. Dabei sind Bürgerinnen und Bürger selbst für den Schutz ihrer digitalen Schnittstellen verantwortlich und damit besonders anfällig für Cyberangriffe.

file://polizei.nrw.de/Home-50/NW048050/cybercrimeBundeslagebild2024_Infografik.pdf

Das sicherste System reicht alleine nicht, wenn die Benutzer und Bürger nicht geschult und/oder achtsam sind.

Neben Angriffsvektoren, die Schwachstellen in Software ausnutzen, sind Phishing-Angriffe¹ eine der häufigsten Methoden, um Zugang zu Systemen zu erhalten.

Diese zielen meistens auf Unaufmerksamkeit der **Benutzer** ab. Das ist eine wichtige Erkenntnis, denn auch technisch versierte Benutzer können Opfer von Phishing werden².

Seit der Existenz von LLMs (Large Language Models) wie ChatGPT, können Angreifer diese Tools nutzen, um überzeugendere Phishing-Nachrichten oder Falschinformationen zu erstellen. Mit Kenntnis des Angreifers von Strukturen und Namen in der Organisation oder des privaten Umfelds des Bürgers, können diese Informationen in die Nachrichten eingebaut werden, um die Glaubwürdigkeit zu erhöhen.

Dieser Angriffsvektor wird daher häufig auch "Social Engineering" genannt, da er die menschliche Psychologie ausnutzt, anstatt technische Schwachstellen. Mit ähnlichem Ansatz verbreiten sich solche Ansätze auch im privaten Bereich. In den sozialen Medien werden echte von KI-Videos kaum noch unterschieden.

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Social-Engineering/social-engineering_node.html

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/3-Tipps-fuer-mehr-IT-Sicherheits-Awareness/3-tipps-fuer-mehr-it-sicherheits-awareness_node.html

II. Gründe für ein DARP der Stadt Unna:

Ein DARP ist Grundlage zur Schaffung eines Problembewusstseins bei den Bürgerinnen und Bürgern und beschäftigt sich zudem auch mit Möglichkeiten zur Schaffung von Achtsamkeit und Resilienz, insbesondere bei stark vulnerablen Bevölkerungsgruppen (Kinder, Jugendliche, Senioren). Ein Programm ermöglicht eine **gezielte Koordination** von weiteren und zusätzlichen Maßnahmen durch ein zu schaffendes **Netzwerk** und eine anschließende Evaluation, um Haushaltsmittel sachgerecht einsetzen zu können. Zudem ermöglicht ein DARP unterschiedliche Einrichtungen und Gremienträger in einem Netzwerk einen Austausch und Abstimmungen vorzunehmen, um Maßnahmen ganzheitlich aufeinander auszurichten und somit **Personal- und**

¹ **Phishing-Angriffe** sind betrügerische Versuche, an sensible Daten wie Passwörter, Kreditkartennummern oder Bankdaten zu gelangen, indem Kriminelle sich als vertrauenswürdige Absender (z.B. Banken, Paketdienste) ausgeben und Opfer dazu verleiten, über gefälschte Links auf Websites ihre Informationen einzugeben oder Malware herunterzuladen

² Zumeist wird in diesen Nachrichten auf Dringlichkeit oder Angst gesetzt, um die Opfer zur schnellen Handlung zu bewegen. Mit einem Klick auf einen Link in der Nachricht, kann Schadsoftware heruntergeladen oder Zugangsdaten auf gefälschten Webseiten abgegriffen werden.

Sachressourcen zu bündeln. Das Ziel ist, dass der Staat bzw. das Land die Rahmenbedingungen und Angebote schafft, die Kommune sie bürgernah einsetzt und die bestehenden Ansätze in Formate und nachhaltige Aktionen bringt, vor Ort. Dies hätte nicht nur für die Stadt Modellcharakter, sondern auch für die Region. Dabei spielt es eine wesentliche Rolle einen **agilen** Ansatz zu verfolgen, da traditionelles Verwaltungshandeln oft zu träge für die digitalen Herausforderungen ist.

1. Erwartete positive Auswirkungen (mit einem DARP):

- Die persönliche Resilienz wird durch Achtsamkeit gestärkt, die die Bürgerinnen und Bürger auf mögliche Szenarien von Cyberangriffen vorbereitet und vor Desinformationen schützt.
- Die Stadt wird bürgernah und kommt der Verantwortung nach, seine Bürgerinnen und Bürger zu schützen und Angebote zu schaffen, sich zu informieren und resilienter zu werden.
- Positive Auswirkungen auf Bildung und Verständnis zur Stadt, Land und Staat sowie zu den Grundlagen unserer Demokratie. Dies mindert die Anfälligkeit für extremistische und radikale Manipulation und Desinformationen.
- Stärkung der demokratischen Kultur in Unna, Verwaltung als Mitgestalter nicht Träger
- Unna könnte mit einem DARP landesweit einen neuen Weg beschreiten und könnte zum best-practise Beispiel für weitere Kommunen werden.
- Zusätzlich könnten Fördermittel akquiriert werden indem sich die Stadt auf Wettbewerbe und Fördertöpfe mit Maßnahmen aus einem DARP bewerben kann (siehe II 1a. und 1b.).

a. Schule und kindliche Bildung

<https://www.schulministerium.nrw/demokratisch-handeln>

<https://www.bpb.de/lernen/angebote/schuelerwettbewerb/>

b. Ganzheitlicher Ansatz

https://www.engagiert-in-nrw.de/landesservicestelle/engagement-und-foerdermittel-von-bis-z/ausgewaehlte-bundesfoerderprogramme#faq_question_4194

<https://www.demokratie-leben.de/>

2. *Erwartete negative Auswirkungen (ohne DARP):*

- Steigende Cybercrimezahlen, schutzlose Bevölkerung, private Insolvenzen
- Einfluss fremder Mächte (z. B. Russland, China, USA) auf die Landtagswahl 2027, Bundestagswahl 2029 sowie Kommunalwahl 2030 durch Falschinformationen
- Erstarben extremistischer Parteien und Positionen
- Einfache Vorbereitung von analogen und digitalen Sabotageaktionen auf kritische Infrastruktur durch Wahrnehmungsdefizite und Unachtsamkeit in der Bevölkerung und Verwaltung

III. Zusammenfassung und Schlussfolgerung

Die Bürgerinnen und Bürger der Stadt Unna sind in der digitalen Welt zunehmend potentiellen Desinformationen und Cyberattacken ausgesetzt. Dabei sind neben der gesamten digitalen Bevölkerung insbesondere auch die vulnerablen Gruppen wie Kinder, Jugendliche und Senioren gefährdet, da sie aus unterschiedlichen Gründen potentielle Opfer oder Empfänger von Desinformationen, kriminellen Machenschaften, Manipulation oder Ausspähungsangriffen sind. Täter und Angreifer haben dabei unterschiedliche Motive. Die Bandbreite reicht dabei von finanzieller Bereicherung hin zur Verunsicherung und Schüren von Angst bis zur Destabilisierung unseres demokratischen Systems durch Beeinflussung von Wahlen oder demokratischen Prozessen. Oft soll dabei das Vertrauen in den Staat und seinen Institutionen geschädigt werden. Zukünftig gilt es die Bürgerinnen und Bürger, insbesondere die o.g. Gruppen vor Angriffen zu schützen und sie für derartige Erscheinungsformen zu sensibilisieren. Die Behörden kommen ihren Aufgaben zum Teil nach, vollumfänglicher Schutz bedarf allerdings einem ganzheitlichen Konzept. In einem ganzheitlichen Konzept kommt der Zivilgesellschaft eine besondere Bedeutung zu. Sie müssen dabei unterstützt werden, ihre Achtsamkeit für Desinformationen, Sabotage und Cyberangriffe zu fördern und resilient zu werden. Dies bedarf einer interdisziplinären Zusammenarbeit und Koordination der kommunalen und landeseigenen Einrichtungen, als auch mit den Trägern zivilgesellschaftlicher und schulischen Institutionen. Die Maßnahmen der Stadt Unna sollten hier zunehmend intensiviert werden.

Zudem Bedarf der Aufbau und die Errichtung von Strukturen für ein DARP Zeitressourcen, die mit Hinblick für die Landtagswahl in 2027 kaum noch vorhanden sind. Daher gilt es bereits im Haushalt der Stadt Unna in 2026 den finanziellen Rahmen bereit zu stellen, um die Bildung von Strukturen zu ermöglichen. Der Schwerpunkt sollte dabei auf den vulnerablen Bevölkerungsgruppen (Kinder, Jugendliche, Senioren) liegen. Auf diese Weise können wir interkommunale Kompetenzen aufbauen, Schulungen anbieten und eine Anlaufstelle schaffen, an die sich Benutzer bei Fragen wenden können, falls ihnen eine Nachricht verdächtig vorkommt. Jugendliche Zielgruppen könnten

durch einen Peer-to-Peer Ansatz³ besser erreicht werden. Sichere Onboarding-Prozesse ermöglichen eine bürgernahe Einführung in die digitale Welt und schafft Sicherheitsbewusstsein in der Bevölkerung. Mögliche Angriffsziele von Cyberattacken und die Auswirkungen müssen Bestandteil von Schulungen und Informationskampagnen sein, damit auch hier die Aufmerksamkeit gegenüber Falschmeldungen und potentiellen Angriffszielen zunimmt.

Schlüsselbegriffe:

Netzwerk, gezielte Koordination, Bündelung von Ressourcen, hybride Bedrohungen, Cyberangriffe auf Nutzer und kritische Infrastruktur, Sabotage, Falschinformation, Hassrede, künstliche Intelligenz, Agilität

Schnittstellen:

VHS, Bevölkerungsschutz, Digitalstrategie, Kriminalprävention, KRITIS, Schulen, Senioren, Jugend, Kultur, Soziales, Vereine, Medien, Politik, Verwaltung

Mit freundlichen Grüßen



Hestia van Roest
Fraktionsvorsitzende
DIELINKE.Volt



Thomas Franta
Fraktionsvorsitzender
DIELINKE.Volt

³ Im sozialen Bereich bedeutet Peer-to-Peer (P2P) Unterstützung oder Lernen „auf Augenhöhe“ durch **Gleichgestellte**, die ähnliche Erfahrungen teilen (z.B. Krankheit, Sucht, Behinderung), um sich gegenseitig zu motivieren, zu beraten und Selbstbestimmung zu fördern, wobei Fachkräfte die Rolle von Begleitern einnehmen und nicht als primäre Experten auftreten. Es geht um den Austausch von Erfahrungen und praktischen Fähigkeiten zwischen Menschen mit gemeinsamem Hintergrund (z.B. in der Aufklärung, Prävention oder Rehabilitation), um das Selbstwertgefühl zu stärken und eine Empathie zu schaffen, die von professionellen Beratern oft nicht erreicht wird. Hier: Jugendliche lernen mit Jugendlichen.