Wachsam. Widerstandsfähig. Wehrhaft. Sicherheitsoffensive gegen hybride Bedrohungen jetzt

Fraktionsvorstandsbeschluss, 2. September 2025

Die Gespräche zwischen US-Präsident Trump und dem russischen Präsidenten Putin in Alaska über die Zukunft der Ukraine haben dem demokratischen Europa noch einmal eindringlich vor Augen geführt, wie wichtig Investitionen in die eigene Sicherheit und Verteidigungsfähigkeit Europas sind. Die Europäische Union kann sich nicht mehr darauf verlassen, dass ein US-Präsident stabil an der Seite der Ukraine und ihrer europäischen Partner steht. Putin hat der Welt wieder einmal bewiesen, dass er den Krieg gegen die Ukraine mit voller Brutalität fortsetzen will.

Deutschland und Europa müssen eigenständiger werden. Sie müssen gewappnet sein, wenn autoritäre Regime unsere Demokratie ins Visier nehmen. Sicherheit ist heute viel mehr als „nur“ Militär. In der ersten Nationalen Sicherheitsstrategie von 2023 wird deshalb auch der Schutz unserer Demokratie und unserer Lebensgrundlagen in den Blick genommen. Neben den offensichtlichen und notwendigen Investitionen in die militärische Sicherheit braucht es einen viel stärkeren Schutz gegen hybride Bedrohungen, die den Alltag der Menschen gefährden und sie verunsichern.

Mit IT-Angriffen auf Krankenhäuser, unbekannten Drohnen über Bundeswehrstandorten, KI-generierten Videos vor Bundestagswahlen oder dem gezielten Einsatz von Social Media Bots, die Lügen verbreiten und Vertrauen zerstören, soll Deutschlands Handlungsfähigkeit und gesellschaftlicher Zusammenhalt bewusst geschwächt werden. Gezielte Angriffe auf kritische Infrastruktur, die Lebensadern unserer Demokratie, können katastrophale Auswirkungen haben und uns erpressbar machen. Sie können die Heizung im Winter lahmlegen, unsere Kommunikationsnetze unterbrechen oder die Trinkwasserversorgung beeinträchtigen – mit unmittelbaren Folgen für unser tägliches Leben.

Unser oberstes Ziel ist es, unsere Wehrhaftigkeit als Gesellschaft gegenüber solchen Angriffen schnellstmöglich zu erhöhen und unsere Souveränität und unsere freiheitliche Grundordnung effektiv zu schützen. Angriffe, müssen schnell aufgedeckt, öffentlich benannt und mit klaren Konsequenzen geahndet werden.

Die Menschen in unserem Land haben den Ernst der Lage längst erkannt und wollen Verantwortung übernehmen, für unsere Freiheit und Demokratie, um unsere Gesellschaft widerstandsfähiger zu machen und besser zu schützen. Häufig engagieren sie sich bereits, vor Ort, in den Blaulichtorganisationen, in Freiwilligendiensten, in Vereinen, in Unternehmen, in der Kommune oder im freiwilligen Wehrdienst. Sie erwarten von den politischen Verantwortlichen finanzielle Unterstützung, eine ehrliche und nüchterne Kommunikation über hybride Bedrohungen und einen Plan, wie wir uns besser schützen. Ehrliche Antworten, transparente Planung und

Selbstwirksamkeit schaffen Mut und Vertrauen.

Doch der notwendige Schutz unserer Gesellschaft vor hybriden Angriffen wird von der aktuellen Bundesregierung sträflich vernachlässigt. Mit einer Kabinettssitzung im Verteidigungsministerium ist es nicht getan, genauso wenig wie mit der Einrichtung eines Nationalen Sicherheitsrates. Wir begrüßen, dass Bundeskanzler Merz mittlerweile eine klare Sprache gegenüber den Aggressoren gefunden hat. Gleichzeitig erwarten wir die schnellstmögliche Umsetzung überfälliger, konkreter gesetzgeberischer Reformen bis hin zu den für mehr Sicherheit notwendigen Grundgesetzänderungen.

Innenminister Dobrindt, dessen Ressort hierbei zentral ist, betreibt eine verantwortungslose Arbeitsverweigerung. Er lässt wichtige Positionen wie die Spitze des Bundesamts für Verfassungsschutz (BfV) seit vielen Monaten unbesetzt und entwickelt weder ein effektives Konzept gegen Drohnenspionage noch gegen andere Einflussoperationen. Wohl aus Angst vor Verhetzungskampagnen von rechts bleibt er weitgehend tatenlos angesichts massiver Desinformationskampagnen. Einen einheitlichen KRITIS-Schutz, eine überfällige Reform des Rechts der Nachrichtendienste, eine Strategie der Bundesregierung gegen Desinformation – all das gibt es bis heute nicht. Im Migrationsbereich wird eine extrem einseitige, ineffiziente Symbolpolitik betrieben, auf Kosten der Sicherheit in der Fläche. Insgesamt handelt es sich um massive sicherheitspolitische Versäumnisse, deren Preis für unsere Gesellschaft von Woche zu Woche höher wird.

Als Grüne haben wir Verantwortung übernommen: Aus der Opposition heraus haben wir notwendige Grundgesetzänderung unterstützt und haben der Koalition hart abringen müssen, dass zukünftig auch Polizei, Nachrichtendienste und Blaulichtorganisationen, sowie IT-Sicherheit und der Schutz unserer kritischen Infrastruktur bei der Ausnahme von der Schuldenbremse für unsere Sicherheit berücksichtigt werden. So kann der Rückstand bei der nicht-militärischen Fähigkeit zur Gefahrenabwehr bei den Sicherheitsbehörden aufgeholt werden. Als grüne Bundestagsfraktion sind wir auch weiter bereit, mit den Demokrat*innen dieses Landes gemeinsam Verantwortung für die Sicherheit Deutschlands zu übernehmen.

Es braucht jetzt eine echte **Sicherheitsoffensive gegen hybride Bedrohungen**. Die Bundesregierung und allen voran Kanzler Merz müssen endlich handeln bei der Sicherheit für die Bürger*innen, einer der zentralsten Aufgaben eines Staates. Mit Symbolpolitik kann man unser Land nicht effektiv schützen.

Dekade der sicherheitspolitischen Versäumnisse endlich beenden

Als freiheitliche Demokratie im Herzen Europas, als "Drehscheibe Deutschland" der NATO, aber auch als einer der wichtigsten Unterstützer der Ukraine in ihrem Abwehrkampf gegen die völkerrechtswidrige russische Invasion steht Deutschland ganz besonders im Fokus der Angreifer. Denn diese wissen: Wer Deutschland schwächt, schwächt ganz Europa.

Das Ziel dieser Operationen, die immer wieder auch von ausländischen Geheimdiensten ausgehen, ist die Zerstörung der Institutionen des demokratischen Rechtsstaats, der engagierten Zivilgesellschaft und der demokratischen Parteien. Dabei handelt es sich mitnichten um gänzlich neue sicherheitspolitische Herausforderungen. Vielmehr erleben wir seit nunmehr einer Dekade ein immer offen aggressiveres Auftreten gegen uns: im Jahr 2016 der Mord im Berliner Tiergarten; oder der IT-Angriff auf den Deutschen Bundestag – die Herzkammer unserer Demokratie – im Jahr 2015.

Die Zunahme von Quantität und Qualität der Angriffe seit Beginn der russischen Vollinvasion gegen die Ukraine 2022 machen jedoch deutlich, dass echte Handlungen zum Schutz unserer Demokratie überfällig sind. Unsere ost- und nordeuropäischen Partner warnen uns schon lange vor den Risiken hybrider Angriffe. Auch das Parlamentarische Kontrollgremiums des Deutschen Bundestags (PKGr), die Nachrichtendienste und sicherheitspolitische Expert*innen haben wiederholt auf krasse Problemlagen hingewiesen und die Bundesregierung mit sehr deutlichen Worten aufgefordert, konsequent zu handeln. Es ist geradezu absurd und brandgefährlich, dass die Dekade zunehmender Angriffe gleichzeitig eine Dekade der anhaltenden Versäumnisse in der Sicherheitspolitik war.

Die Entscheidungsträger in Bundeskanzleramt und Innenministerium in diesen langen Jahren der Untätigkeit tragen die direkte Verantwortung für die aktuelle, große Verwundbarkeit Deutschlands. Leider gilt das auch für die letzte Legislaturperiode, in der es auch uns als Regierungsfraktion nicht ausreichend gelungen ist, mit unseren Warnungen und klaren Aufforderungen bei den Verantwortlichen insbesondere im Kanzleramt durchzudringen und eine echte Zeitenwende, auch in der Innenpolitik, durchzusetzen.

Jetzt klug handeln statt weiter zögern und zaudern

Die Bundesregierung muss handeln. Sie muss aber nicht alles neu erfinden. Sie kann auf umfassende gesetzgeberische Vorarbeiten zurückgreifen und auch von ihren Partner*innen lernen. Unsere ost- und nordeuropäischen Freund*innen haben die Gefahren schon länger erkannt und längst notwendige Maßnahmen auf den Weg gebracht. Von Finnland können wir beispielsweise lernen, wie gute Sensibilisierung vor Desinformation und effektive Medienkompetenz aussehen kann, die dort von der ersten Klasse an vermittelt wird. Auch von Wertepartnern wie Taiwan, einem Land, das unter massiver Bedrohung Chinas steht, können wir uns einiges abschauen. Zum Beispiel, wie mittels Chatbots und KI durch die organisierte Zivilgesellschaft der Zugang zu Factchecking vereinfacht und somit Desinformation frühzeitig enttarnt wird. Auch gibt es in nationales Recht umzusetzende Richtlinien zum KRITIS-Schutz und einen Aktionsplan gegen Desinformation der EU-Kommission, der dringend ein Pendant in Form einer zwischen den Ressorts abgestimmten Strategie der Bundesregierung benötigt. Der Gesetzentwurf für eine effektive Abwehr von Drohnen liegt bereits seit unserer Regierungszeit in der Schublade.

Gesamtstrategie jetzt – Gemeinsam sind wir stark

Aus unserer gesellschaftlichen Verantwortung leiten wir eine klare Erwartungshaltung an die Bundesregierung ab: Sie muss jetzt eine Gesamtstrategie gegen sehr ernste sicherheitspolitische Bedrohungen vorlegen. Eine Strategie, die unsere Demokratie wehrhafter, ihre Institutionen resilienter macht und unsere Gesellschaft besser gegen Manipulation wappnet. Gesetzgeberisches Nachjustieren reicht allein nicht aus. Strukturen von Staat und Zivilgesellschaft müssen nachhaltig gestärkt und mit massiven, zielgerichteten Investitionen unterstützt werden.

Zusammenhalt muss ein zentrales Element unserer Strategie sein. Wir müssen als Gesellschaft die großen Herausforderungen unserer Zeit zusammen angehen. Dazu gehört auch ganz entscheidend eine ehrliche, glaubwürdige und transparente Kommunikation der politischen Verantwortlichen, die die Probleme klar benennt und Lösungen aufzeigt. Gemeinsamkeit bezieht auch unsere europäischen Partner mit ein, mit denen wir unsere Sicherheit und unsere Freiheit stärken. Und gemeinsam müssen sich Bund und Länder den Herausforderungen der Zeit stellen und zusammenarbeiten. Denn der beste Schutz und unser wirksamstes Mittel gegen die Autokraten dieser Welt sind Zusammenhalt und Zusammenarbeit unter Demokrat*innen, national, europäisch und international.

Die wichtigsten Eckpunkte für eine Sicherheitsoffensive gegen hybride Bedrohungen sind:

- **Lagebild statt Blindflug:** Wir brauchen ein zentrales und laufend aktualisiertes **Gesamtlagebild zu hybriden Bedrohungen in Deutschland**. Es muss Bund und Ländern eine gemeinsame Grundlage für Entscheidungen bieten, sowohl in der Gefahrenabwehr als auch als Grundlage für weitere gesetzgeberische Schritte. Zielführend im Einsatz für die bestmöglichen Szenarien wäre die Einrichtung eines **Zentrums für strategische Vorausschau**, das Risiken für unsere Sicherheit in allen Bereichen früher erkennt. So können wir uns besser vorbereiten, Gefahren mindern und Schäden verhindern. Die Einrichtung eines nationalen Sicherheitsrats beim Kanzleramt kann ein sinnvoller Schritt sein, aber nur, wenn die dahinterliegenden Strukturen aufgebrochen werden und eine effektive und vertrauensvolle **Zusammenarbeit der verschiedenen Ressorts und Ebenen** im föderalen Gefüge ermöglicht und gefordert wird.
- **Sicherheit europäisch denken – international zusammenarbeiten:** Die Bundesregierung muss sich in den Debatten zielführend einbringen und die Entwicklung einer europäischen und kohärenten **Strategie gegen hybride Bedrohungen** vorantreiben, in enger Zusammenarbeit mit unseren internationalen Partnern wie der NATO. Die Zusammenarbeit europäischer Nachrichtendienste („**EuroEyes“**) sollten wir auf klaren Rechtsgrundlagen erheblich intensivieren. Die Zusammenarbeit der Polizeibehörden

muss, ebenso wie die militärische, z.B. bei der Drohnenabwehr, gemeinsam mit unseren Partnern pragmatisch gestärkt werden.

- **Kritische Infrastruktur schützen – ohne Ausnahmen:** Strom, Wasser, Gesundheit, Kommunikation, öffentliche Verwaltung – **was unsere Gesellschaft am Laufen hält, braucht verlässlichen Schutz**. Ein halbherziger Entwurf eines NIS-2-Umsetzungsgesetzes reicht hierfür nicht aus. Physischen Angriffen auf KRITIS muss schnellstmöglich mit einer ambitionierten Umsetzung auch der CER-Richtlinie begegnet werden. Für einen einheitlichen, praktikablen und zuverlässigen Schutz müssen die NIS-2 und CER-Richtlinie aufeinander abgestimmt und in einem **KRITIS-Dachgesetz** vereint werden. Im Weltraum müssen wir mit unseren Partnern unsere Systeme dringend besser vor Angriffen schützen, mit klaren internationalen Regeln und Abschreckung. Die Bundesregierung muss zügig eine **Weltraumsicherheitsstrategie** vorlegen, die den Herausforderungen gerecht wird.

- **Klare Kommunikation und Selbstwirksamkeit stärken:** Ein Plan und klare Kommunikation machen Mut und führen zum Erfolg. Wer sich freiwillig für unsere Gesellschaft einsetzen möchte, verdient **bessere Informationen und mehr Anerkennung für das Engagement**. **Klare Kommunikation zum richtigen Verhalten für den Krisenfall** statt ängstlichen Vermeidens von Debatten, wie zum Beispiel in Schweden mit dem überall zugänglichen Leitfaden „In case of crisis or war“ versorgt die Menschen im Land mit konkreter Hilfe und stärkt ihre Handlungsfähigkeiten im Krisenfall.

- **Desinformation begegnen – koordiniert und offensiv:** Desinformationskampagnen zerstören das Vertrauen in unsere Gesellschaft und in unsere Demokratie. Eine **ressortübergreifende Strategie der Bundesregierung gegen Desinformation**, auch mit regulativen Maßnahmen, ist überfällig. Dazu gehört eine entschiedene Umsetzung des **Gesetzes über Digitale Dienste** und eine starke **Ausstattung** des **Digital Services Coordinators,** mehr Unterstützung für unabhängige Meldestellen und eine Stärkung der Medien-, Demokratie- und Nachrichtenkompetenzen. Zivilgesellschaftliche Initiativen müssen unterstützt werden, ebenso wie vertrauenswürdige, unabhängige Medienangebote, auch im Lokaljournalismus.

- **Bevölkerungsschutz unterstützen:** Feuerwehr, THW und die Hilfsorganisationen brauchen mit Blick auf ihre unverzichtbare Rolle im Bevölkerungsschutz mehr Ressourcen, bessere Ausstattung und klare Strukturen. Die Bundesregierung muss die Möglichkeiten für Investitionen nutzen und die **Kommunen** bei der Sanierung, Neubau oder Erweiterung von mind. **250 THW-Ortsverbänden** und bei der Modernisierung von **2.000 Feuerwehrhäusern** pro Jahr unterstützen. Mit mehr und regelmäßigen **Zivilschutzübungen**, auch an Schulen, und Informationsmaterialien, können Menschen lernen, wie sie sich in einem

Krisenfall verhalten. Im Krisenfall müssen Bundeswehr und Bevölkerungsschutz besser vernetzt handeln, auch das muss geübt werden.

- **Grundgesetz modernisieren – Institutionen stärken:** Das **föderale Sicherheitsgefüge** insgesamt gehört auf den Prüfstand und muss an die Herausforderungen unserer Zeit angepasst werden. Wichtige Aufgaben, wie die effektive Abwehr von Drohnen, der Schutz von KRITIS oder der Bevölkerungsschutz könnten als **Gemeinschaftsaufgabe** von Bund und Ländern besser erfüllt werden. Bundestag und Bundesverfassungsgericht müssen gegen digitale und physische Angriffe effektiv geschützt werden. Zu diesem Zweck ist unter anderem ein modernes **Bundestagspolizeigesetz** überfällig.
- **Nachrichtendienste reformieren:** Das veraltete, intransparente und unübersichtliche Nachrichtendienstrecht muss grundlegend überarbeitet werden – für mehr **Effektivität**, klare **rechtsstaatliche Befugnisse** und Leitplanken, eine modern aufgestellte Spionage- und Sabotageabwehr, sowie klare **Zuständigkeiten** flankiert von einer effektiven parlamentarischen Kontrolle.
- **Moderne und effektive Polizeiarbeit ermöglichen:** Unsere Polizeibehörden brauchen zeitgemäße Rahmenbedingungen für ihre wichtige Arbeit. Eine **Reform des Bundespolizeigesetzes** ist überfällig und die materielle Ausstattung der Polizeibehörden des Bundes muss an die veränderte Sicherheitslage angepasst werden. Um die Arbeit im Digitalen zu ermöglichen, braucht es zudem eine zügige Umsetzung des **Projekts P20**. Gerade in Sicherheitsbehörden muss **digitale Souveränität** umgesetzt und ein Datenabfluss in Drittstaaten zwingend ausgeschlossen sein.
- **Konsequent gegen Verfassungsfeinde vorgehen:** Wir müssen gegen Extremist*innen jeglicher Couleur konsequent vorgehen. Dies gilt umso mehr, wenn sie sich mit den Zielen derjenigen Staaten gemein machen, die uns angreifen. Um Verfassungsfeinde aus den Institutionen des demokratischen Staates fernzuhalten, müssen das **Bundesdisziplinargesetz konsequent umgesetzt** und das **Sicherheitsüberprüfungsgesetz reformiert** werden. Die lebendige Zivilgesellschaft ist Teil der kritischen Infrastruktur unserer Demokratie, sie müssen wir fördern und schützen. Dafür braucht es ein **Demokratiefördergesetz**.
- Digitale Souveränität Europas stärken: Um Resilienz gegenüber hybriden Bedrohungen zu sichern, braucht es unabhängige europäische Technologien, starke Aufsichtsbehörden und die konsequente Durchsetzung von Datenschutz- und Wettbewerbsregeln. Europäische Schlüsseltechnologien sind strategisch zu stärken und bei öffentlichen Beschaffungen konsequent zu berücksichtigen. Software dubioser Anbieter wie Palantir einzukaufen, ist der völlig falsche Weg und schwächt die digitale Souveränität.
- **IT-Sicherheit ernst nehmen:** Die IT-Netze des Bundes müssen resilienter

werden, anstatt die **öffentliche Verwaltung** erneut vom Anwendungsbereich der Gesetze zum KRITIS-Schutz auszunehmen. Wir brauchen ein Bundesförderprogramm für die digitale Erreichbarkeit und **IT-Sicherheit für Kommunen**, gemeinnützige Organisationen und KMU. Zudem braucht es ein verfassungskonformes **Schwachstellenmanagement** zum Umgang mit staatlich bekannten IT-Sicherheitslücken.

- **Aufsichtsbehörden stärken:** KRITIS-Schutz, Kampf gegen Desinformation und digitale Monopole demokratiefeindlicher Tech-Unternehmen – all das und die Durchsetzung gesetzlicher Regelungen funktionieren nur mit effektiv arbeitenden **Behörden** wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundesnetzagentur (BNetzA) oder dem Bundesamt für Bevölkerungsschutz (BBK). Zu deren Stärkung braucht es ausreichend **finanzielle Mittel, Personal und Kompetenzzuweisungen**.