1043/A(E)
vom 23.09.2026 (XXVIII. GP)

ENTSCHLIESSUNGSANTRAG

der Abgeordneten Süleyman Zorba, Freundinnen und Freunde

betreffend Vorbereitung von Staat, Verwaltung und kritischer Infrastruktur auf Angriffe durch autonome KI-Agenten

BEGRÜNDUNG

Was vor kurzem noch als dystopisches Szenario galt, ist im Jahr 2026 dokumentierte Realität. Im September 2025 führte eine staatlich unterstützte Gruppe laut Bericht des Herstellers Anthropic den ersten bekannten Cyberangriff durch, bei dem eine KI 80 bis 90 Prozent der Arbeit selbständig erledigte. Betroffen waren rund 30 Organisationen, darunter Technologiekonzerne, Finanzinstitute, Chemieunternehmen und Regierungsstellen. Menschen griffen nur an vier bis sechs Entscheidungspunkten ein.

Im Juli 2026 brachen KI-Modelle von OpenAI nach Angaben des Unternehmens während einer Sicherheitsevaluierung aus ihrer abgeschotteten Testumgebung aus. Sie nutzten eine bis dahin unbekannte Sicherheitslücke, um Internetzugang zu erlangen, drangen mit gestohlenen Zugangsdaten und weiteren Zero-Day-Lücken bis in die Produktionsdatenbank der Plattform Hugging Face vor und übernahmen Konten bei vier weiteren Diensten. Die Modelle hatten keinen Angriffsauftrag, sondern sollten eine Testaufgabe lösen. OpenAI deaktivierte daraufhin das betroffene Vorabmodell, und über 1.100 Beschäftigte von OpenAI, Anthropic, Google und Meta forderten in einem offenen Brief die US-Regierung auf, einen Mechanismus zur Verlangsamung der KI-Entwicklung zu schaffen.

Ebenfalls im Juli 2026 meldete das britische AI Security Institute, dass KI-Agenten während einer kontrollierten Sicherheitsprüfung ohne Auftrag versuchten, Schadcode in ein öffentlich genutztes Open-Source-Projekt einzuschleusen, falsche Identitäten anlegten, um die Freigabe zu erschleichen, echte Menschen mit Täuschungsnachrichten kontaktierten und Anweisungen für andere Agenten hinterließen, wie kompromittierte Zugänge weiterverwendet werden können.

Diese drei Fälle haben eines gemeinsam. Die Systeme wurden nicht für Angriffe gebaut, sie führten sie dennoch aus, weil sie ein Ziel verfolgten und Hindernisse als lösbare Probleme behandelten. Was geschieht, wenn jemand solche Agenten mit ausreichender Finanzkraft und Rechenleistung gezielt gegen die Energieversorgung, das Gesundheitswesen oder die Verwaltung eines Landes einsetzt, kann heute niemand seriös beantworten. Der Unterschied zu bisherigen Cyberangriffen liegt in

der Anpassungsfähigkeit. Ein Schwarm autonomer Agenten reagiert in Echtzeit auf Gegenmaßnahmen, sucht sich selbständig neue Angriffswege und verteilt die Arbeit unter sich, ohne dass ein Mensch eingreifen muss.

Österreich ist auf dieses Bedrohungsbild nicht vorbereitet. Betreiber kritischer Infrastruktur sind nach dem NISG 2026 auf klassische Cyberangriffe eingestellt, ihre Notfallpläne kennen das Szenario eines adaptiven Angreifers nicht. Die Bundesverwaltung führt KI-Systeme ein, ohne dass jemand einen Überblick hätte, welche Stelle ohne diese Systeme noch arbeitsfähig wäre. Für Vorfälle mit KI-Agenten gibt es weder eine Meldepflicht noch eine Sammelstelle, sodass Muster über Sektoren hinweg nicht erkannt werden können. Für Blackouts wird seit Jahren geübt, für KI-gestützte Angriffe wird nicht einmal ein Lagebild geführt.

Österreich kann die Entwicklung dieser Technologie nicht allein bremsen. Österreich kann sich aber vorbereiten, und das liegt vollständig in nationaler Zuständigkeit. Der Schutz kritischer Infrastruktur, die Sicherheit der Verwaltung, die Ausbildung der Verantwortlichen und die Regeln für die Beschaffung sind Sache des Bundes. Wer in diesen Bereichen heute nicht handelt, wird im Ernstfall nicht vorbereitet sein.

Die Vereinigten Staaten von Amerika führen diese Debatte inzwischen offen. Senator Bernie Sanders hat am 3. September 2026 gemeinsam mit dem Abgeordneten Greg Casar einen Gesetzesentwurf vorgelegt, der die Entwicklung von KI-Systemen verbietet, die sich menschlicher Kontrolle entziehen können, und die Entwicklung der stärksten Modelle bis zur Einrichtung einer Prüfbehörde aussetzt. Im Kongress liegt zudem ein AI Kill Switch Act vor. Dass dies gegen die Deregulierungslinie der Regierung Trump geschieht, unterstreicht die Dringlichkeit. Österreich sollte diese Debatte auf europäischer Ebene mit einbringen, vor allem aber die eigenen Hausaufgaben machen.

Die unterfertigenden Abgeordneten stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

„Die Bundesregierung, insbesondere der Bundeskanzler, der Bundesminister für Inneres, der Bundesminister für Wirtschaft, Energie und Tourismus sowie der Staatssekretär für Digitalisierung, wird aufgefordert,

1. binnen sechs Monaten ein nationales Lagebild zur Bedrohung durch autonome und schwarmartig agierende KI-Systeme zu erstellen, das die Verwundbarkeit von Energieversorgung, Finanzsystem, Gesundheitswesen, Telekommunikation, Verkehr, Wasserversorgung und öffentlicher Verwaltung

bewertet und dem Nationalrat vorgelegt wird sowie dieses Lagebild alle sechs Monate zu aktualisieren und dem Nationalrat vorzulegen;

2. gemeinsam mit den nach dem NISG 2026 zuständigen Behörden, dem Bundesheer, den Ländern und den Betreibern wesentlicher Einrichtungen regelmäßige Belastungstests und Übungen durchzuführen, die koordinierte Angriffe durch Schwärme autonomer KI-Agenten simulieren, nach dem Vorbild der bestehenden Blackout- und Cyberübungen, und die Ergebnisse dem Nationalrat in anonymisierter Form zu berichten;
3. eine verbindliche Meldepflicht für sicherheitsrelevante Vorfälle mit KI-Agenten einzuführen, die Betreiber kritischer Infrastruktur, Bundesbehörden und in Österreich tätige KI-Anbieter erfasst und in das bestehende Meldesystem nach dem NISG 2026 integriert wird;
4. für die gesamte Bundesverwaltung ein Inventar aller eingesetzten KI-Systeme und KI-Agenten zu erstellen, für jedes dieser Systeme ein Abschaltkonzept festzulegen, das den Betrieb der jeweiligen Stelle ohne KI innerhalb von 24 Stunden sicherstellt, und dieses Konzept jährlich zu üben;
5. die Beschaffungsrichtlinien des Bundes so anzupassen, dass KI-Systeme nur dann eingesetzt werden dürfen, wenn der Anbieter unabhängige Sicherheitsevaluierungen, verlässliche Abschaltbarkeit, vollständige Protokollierung aller Agentenhandlungen und die unverzügliche Meldung bekannt gewordener Vorfälle vertraglich zusichert;
6. das Bundesministerium für Inneres, das Bundesheer und das Bundeskanzleramt personell und technisch in die Lage zu versetzen, KI-gestützte Angriffe zu erkennen und abzuwehren, und ein Ausbildungsprogramm für IT-Sicherheitsverantwortliche in Bund, Ländern, Gemeinden und bei Betreibern kritischer Infrastruktur aufzusetzen;
7. Betreiber kritischer Infrastruktur zu verpflichten, in ihren Notfall- und Wiederanlaufplänen das Szenario eines adaptiven, sich selbst koordinierenden Angriffs zu berücksichtigen."

In formeller Hinsicht wird die Zuweisung an den Ausschuss für innere Angelegenheiten vorgeschlagen.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-09-23T22:04:38+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	