

22.32

Abgeordneter Süleyman Zorba (Grüne): Danke, Herr Präsident! Frau Präsidentin! Ich spreche wie zu erwarten zu Cybercrime: Danke für den Bericht. Seit der Prüfung und dem Bericht hat sich ja einiges getan. Es gibt Empfehlungen, die umgesetzt worden sind, es gibt Empfehlungen, an denen noch gearbeitet werden muss. Aber eines hat sich seit der Prüfung gravierend verändert, nämlich die Gefahrenlage, was Cybersicherheit und Cybercrime betrifft, die ist nämlich deutlich schwieriger und schlechter geworden.

Wir kennen alle diese Horrormeldungen aus den vergangenen Wochen, wo auch die Bosse der KI-Konzerne vor ihren Entwicklungen warnen. Jetzt kann man zu dem stehen, wie man möchte: Ist es Marketing, ist es kein Marketing? Eines steht aber fest: Wir müssen gar nicht so weit in die Zukunft schauen, um Gefahrensituationen zu sehen, denn auch heutige Modelle und KI-Technologien, die bestehen, können zu einem Problem werden, nämlich ganz speziell im Cybersicherheitsbereich. *(Beifall bei den Grünen.)*

Wer sich mit Cybersicherheit auseinandersetzt, muss auch festhalten, dass wir in Österreich da nicht immer einen sehr guten Zugang dazu gehabt haben, dass wir da noch einige Dinge aufzuarbeiten haben. Das wird jetzt eben zu einem Riesenproblem. Das erkennt man, wenn man sich vorstellt, zu welchen Problemen das führen kann, wenn Gruppen von KI-Agenten gezielt, konzentriert Sicherheitslücken aufsuchen. Wir haben also das Problem, dass durch den Einsatz von künstlicher Intelligenz Cyberangriffe immer problematischer werden, und auf der anderen Seite haben wir große offene Flanken im Bereich der Cybersicherheit.

Was heißt das für uns? Was heißt das für unsere Systeme? – Egal ob es um den privaten Bereich, die Wirtschaft oder unsere kritischen Infrastrukturen geht, seien es jetzt hybride Kriegssituationen oder auch Gruppierungen mit viel Geld und Ressourcen, die uns da angreifen: Wir haben ein sehr, sehr großes Problem.

Ich möchte jetzt zu dieser Stunde niemandem allzu große Angst machen. Deshalb komme ich mit einem Lösungsvorschlag. Wir haben dazu einen Antrag vorbereitet, mit dem wir viele dieser Punkte aufgreifen könnten. Ich lese ihn vor:

RN/224.1

Entschließungsantrag

der Abgeordneten Süleyman Zorba, Kolleginnen und Kollegen betreffend
„Dringende Vorbereitung von Staat, Verwaltung und kritischer Infrastruktur auf Angriffe durch autonome KI-Agenten“

Der Nationalrat wolle beschließen:

„Die Bundesregierung wird aufgefordert,

1. die Bedrohung durch autonome, schwarmartig agierende KI-Systeme für kritische Infrastruktur systematisch binnen 6 Monaten zu erfassen und in der Folge halbjährlich zu aktualisieren und dem Nationalrat darüber zu berichten,
2. durch Übungen und Belastungstests die Abwehrfähigkeit gegen koordinierte KI-Angriffe zu erproben,
3. eine verbindliche Meldepflicht für sicherheitsrelevante KI-Vorfälle einzuführen und in das Meldesystem nach dem NISG 2026 zu integrieren,

4. ein bundesweites Inventar aller eingesetzten KI-Systeme samt geübtem Abschaltkonzept zu erstellen,
5. die Beschaffung von KI-Systemen an strenge Sicherheits-, Melde-, Protokollierungs- und Abschaltbarkeitsanforderungen zu binden,
6. die Sicherheitsbehörden personell und technisch zur Erkennung und Abwehr solcher Angriffe zu befähigen sowie entsprechende Schulungsprogramme aufzusetzen, und
7. Betreiber kritischer Infrastruktur zu verpflichten, das Szenario eines adaptiven, selbstkoordinierenden Angriffs in ihre Notfallplanung aufzunehmen.“

Ich hoffe auf eine breite Zustimmung. – Danke schön. *(Beifall bei den Grünen und bei Abgeordneten der SPÖ.)*

22.35

Der Gesamtwortlaut des Antrages ist unter folgendem Link abrufbar:

RN/224.2

[Dringende Vorbereitung von Staat, Verwaltung und kritischer Infrastruktur auf Angriffe durch autonome KI-Agenten \(219/UEA\)](#)

Präsident Dr. Walter Rosenkranz: Der soeben vorgetragene Entschließungsantrag ist ordnungsgemäß eingebracht, ausreichend unterstützt und steht daher mit in Verhandlung.

Als Nächste zu Wort gemeldet: Frau Abgeordnete Sunitsch. 3 Minuten eingemeldete Redezeit. – Bitte schön.