BULLETIN DER BUNDESREGIERUNG

Nr. 65-1 vom 25. Juni 2026

Rede des Bundesministers des Innern, Alexander Dobrindt,

zur Stärkung der Cybersicherheit
vor dem Deutschen Bundestag
am 25. Juni 2026 in Berlin:

Sehr geehrter Herr Präsident!
Verehrte Kolleginnen und Kollegen!

Heute bereiten wir einem Meilenstein der Sicherheitsarchitektur in Deutschland den Weg. Mit diesem Gesetzentwurf legen wir schlichtweg den Schalter um: von der Aufklärung hin zur Abwehr. Wir legen die Grundlagen für die aktive Cyberabwehr. Wir machen damit unmissverständlich deutlich: Deutschland handelt entschlossen, wenn es um die Verteidigung im Cyberraum geht.

Cyberangriffe sind nicht neu. Aber wir verändern den Umgang mit den Urhebern, mit den Tätern dieser Cyberattacken. Wer uns zukünftig im Cyberraum angreift, der muss wissen: Wir schlagen zurück und sind in der Lage, die Angreifer in ihrer Infrastruktur zu stören und zu zerstören.

Ich will mich ausdrücklich bei den Kolleginnen und Kollegen in der Koalition für die Beratungen in den vergangenen Monaten und bei allen, die mitgewirkt haben, bedanken, im Besonderen bei der Bundesjustizministerin Stefanie Hubig für die exzellente und konstruktive Zusammenarbeit. Wir zeigen wieder einmal, dass wir hier gemeinsam die Voraussetzungen schaffen, damit unsere Sicherheitsbehörden technisch und rechtlich in der Lage sind, den Bedrohungen standhalten zu können. Dieses Gesetz zur aktiven Cyberabwehr ist eine neue Säule in unserer Sicherheitsarchitektur. Es stärkt das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundeskriminalamt und die Bundespolizei. Und es ist zwingend notwendig, um gegen die immer weiter steigende hybride Bedrohung vorzugehen.

Wir sind täglich Zielscheibe digitaler Angriffe, weil wir als starke Wirtschaftsnation in der Welt unterwegs sind, weil wir ein innovativer Industriestandort sind, weil wir das Zentrum der europäischen Verteidigungsarchitektur darstellen, weil wir ein Wissenschaftszentrum sind. Wir stehen eben im Fokus von professionellen und perfiden Angreifern. Es geht um Spionage, Sabotage und Destabilisierung. Es geht um Einflussnahme und Manipulation. Es geht um die hybride Bedrohung.

Das, was wir täglich erleben, ist der Schattenkrieg des 21. Jahrhunderts. Es ist kein heißer Krieg, aber eine dunkle Bedrohung, die versucht, sich manipulativ über unser Land zu legen. Wir sagen deutlich: Kriminelle Netzwerke, staatliche oder halbstaatliche Akteure, fremde Mächte lassen wir nicht zu. Die Schattenkrieger kriegen heute ein deutliches Signal von uns: Wer uns angreift, der kann darauf vertrauen, dass wir nicht einfach zusehen, sondern zurückschlagen.

Wir stärken unsere Fähigkeiten. Wir stoppen unsere Angreifer. Wir stören ihre Möglichkeiten. Dabei geht es natürlich auch um Prävention; die bleibt unverzichtbar. Wir haben das NIS-2-Gesetz verabschiedet. Wir bauen das BSI weiter auf. Wir bauen resiliente IT-Strukturen auf. Ja, Prävention ist nach wie vor zwingend notwendig, aber sie allein genügt eben nicht. Aktive Cyberabwehr muss ein Bestandteil der deutschen Sicherheitsarchitektur sein.

Ich habe in den vergangenen Tagen immer wieder Vorwürfe gelesen, wir würden einen Hackback initiieren wollen. Das, was wir tun, hat mit einem Hackback beileibe überhaupt nichts zu tun. Ein Hackback bedeutet nämlich, dass man, wenn ein Angreifer seine Attacken beispielsweise gegen unsere Krankenhausinfrastruktur richtet, um diese lahmzulegen, aus Rachegelüsten beispielsweise gegen seine Energieinfrastruktur einen Gegenschlag richtet. Darum geht es schlichtweg nicht. Uns geht es darum: Wer meint, er könnte unsere Infrastruktur, beispielsweise unsere Krankenhausinfrastruktur, aktiv angreifen, der muss einfach damit rechnen, dass wir seine Angriffsarchitektur stören und zerstören. Das ist kein Hackback. Das ist eine angemessene Antwort auf hybride Bedrohungen. Das ist aktive Cyberabwehr. Herzlichen Dank.

* * * * *