bitkom

Stellungnahme

Juni 2025

Aufstellung des Nationalen Sicherheitsrats

Die Fraktionen von Union und SPD haben sich für die 21. Legislaturperiode auf die Einrichtung eines Nationalen Sicherheitsrats im Bundeskanzleramt verständigt. Im Koalitionsvertrag vom 9. April 2025 heißt es dazu:

»*Wir entwickeln den Bundessicherheitsrat, im Rahmen des Ressortprinzips, zu einem Nationalen Sicherheitsrat im Bundeskanzleramt weiter. Er soll die wesentlichen Fragen einer integrierten Sicherheitspolitik koordinieren, Strategieentwicklung und strategische Vorausschau leisten, eine gemeinsame Lagebewertung vornehmen und somit das Gremium der gemeinsamen politischen Willensbildung sein.*« Ergänzend wird vereinbart: »*Für eine ganzheitliche Bewältigung von Krisen braucht Deutschland einen Bund-Länder- und ressortübergreifenden Nationalen Krisenstab der Bundesregierung und ein Nationales Lagezentrum im Bundeskanzleramt, in dem ressortübergreifend ein Gesamtlagebild zusammengefügt wird.*«

Bisher ist der Bundessicherheitsrat (BSR) ein Kabinettsausschuss der Bundesregierung, der für die strategische Ausrichtung und Koordinierung der deutschen Sicherheitspolitik zuständig ist. Die Gründung des Gremiums geht auf einen Kabinettsbeschluss vom 6. Oktober 1955 zurück. Beratungen des BSR finden nicht regelmäßig statt und unterliegen der Geheimhaltung. Den Vorsitz führt der Bundeskanzler, ständige Mitglieder sind unter anderem die Bundesministerinnen und Bundesminister des Auswärtigen, der Verteidigung, des Innern, der Finanzen, der Justiz, für Wirtschaft und Klimaschutz sowie der Chef des Bundeskanzleramts. Weitere Ressorts oder externe Funktionsträger können bei Bedarf hinzugezogen werden.

Angesichts neuer sicherheitspolitischer Herausforderungen ist die Weiterentwicklung des Bundessicherheitsrats zu einem Nationalen Sicherheitsrat im Bundeskanzleramt ein notwendiger Schritt, um sicherheitspolitische Entscheidungen künftig strategischer und technologieadäquater zu treffen. Die sicherheitspolitischen Herausforderungen der Gegenwart – von geopolitischen Spannungen in einer multipolaren Welt bis hin zu hybriden Angriffen auf kritische Infrastrukturen – verlangen nach einer koordinierten und vorausschauenden Antwort auf Bundesebene. Entscheidend für den Erfolg wird sein, ob das Gremium in der Lage ist, Sicherheitspolitik mit einem gesamtstaatlichen Ansatz verlässlich, schnell und ressortübergreifend zu koordinieren und damit im

71%

der Deutsche gehen davon aus, dass Kriege in Zukunft überwiegend auch mit digitalen Mitteln geführt werden. (Bitkom, 2025)

Zusammenwirken zu verbessern. Unsere internationalen Partner benötigen eine klare Ausrichtung Deutschlands – nicht nur im klassisch militärischen Sinne.

Wichtig ist aus Sicht der Digitalwirtschaft, dass ein integrierter und ganzheitlicher Sicherheitsbegriff zugrunde gelegt wird. Die sicherheitspolitische Domäne ist längst über den militärischen und außenpolitischen Blickwinkel hinausgewachsen. Für die sicherheitspolitische Aufstellung Deutschlands und ihrer Partner sind auch andere Faktoren relevant. Dazu zählen unter anderem Energie- und Rohstoffsicherheit, sichere Kommunikationsmöglichkeiten für den Staat und die Behörden, bildungspolitische Weichenstellungen sowie der Abbau technologischer Abhängigkeiten. Vor allem stellen heute aber Cyberangriffe, hybride Einflussoperationen und digitale Sabotageakte eine der zentralen Bedrohungen für Staat, Wirtschaft und Gesellschaft dar. Der deutschen Wirtschaft entstehen jährlich Schäden in Höhe von rund 178,6 Milliarden Euro allein durch Cyberangriffe – ein Ausmaß, das den Handlungsdruck verdeutlicht. Dazu muss der Nationale Sicherheitsrat die digitale Gefahrenlage sowie den Cyber- und Informationsraum systematisch in seine Analysen und Entscheidungsprozesse einbeziehen.

Im Sinne einer integrierten Sicherheitsarchitektur ergeben sich vier zentrale Forderungen an die Ausgestaltung des Nationalen Sicherheitsrats:

1. **Einbindung zentraler Akteure der digitalen Sicherheit**
   Für eine realitätsnahe und wirksame Sicherheitssteuerung muss der Nationale Sicherheitsrat auch die Expertise von Nachrichtendiensten, dem BSI, der BDBOS sowie dem BMDS systematisch einbeziehen. Auch ein Einbezug des Nationalen Cybersicherheitsrats sollte in Betracht gezogen werden. Nur unter Einbezug aller relevanten Akteure lassen sich physische, digitale und hybride Bedrohungen ganzheitlich bewerten und wirksam adressieren.

2. **Kooperation zwischen Staat und Wirtschaft ausbauen**
   Sicherheitspolitische Entscheidungen haben heute mehr denn je auch Auswirkungen auf die Wirtschaft. Gerade im Bereich der Cybersicherheit ist die Zusammenarbeit zwischen Behörden und der Wirtschaft entscheidend. Unternehmen betreiben große Teile der kritischen Infrastrukturen und verfügen über eigenes Lagewissen. Eine engere Verzahnung – etwa durch die formalisierte Einbindung von Wirtschaftsvertreterinnen und -vertretern in beobachtender Funktion – kann helfen, die Perspektiven der Wirtschaft in die sicherheitspolitische Lagebewertung einzubringen und die Fähigkeiten der Wirtschaft zu nutzen und im Sinne einer nationalen Sicherheitsstrategie auszubauen. Notwendige digitale Schlüsseltechnologien werden auch zukünftig überwiegend nicht allein durch den Staat geschaffen, sondern durch eine Wirtschaft, die die Überlegungen eines Nationalen Sicherheitsrates kennt und unterstützt.

3. **Nationales Cyberlagebild als Entscheidungsgrundlage verankern**
   Der Nationale Sicherheitsrat sollte seine Arbeit auf ein konsolidiertes Cyberlagebild stützen können, das alle relevanten öffentlichen Stellen sowie privatwirtschaftliche Akteure umfasst. Ziel muss es sein, Bedrohungslagen in Echtzeit zu erfassen, Informationen gezielt zu teilen und im Krisenfall koordiniert zu handeln. Ein solches Lagebild darf jedoch keine Einbahnstraße sein, sondern muss auch einen Rückkanal für die Akteure etablieren. Derzeit sind Unternehmen gezwungen, auf kommerzielle

Threat-Intelligence-Angebote – häufig aus dem Ausland – zurückzugreifen, von deutschen Behörden erhalten sie kaum verwertbare Informationen. Für eine resiliente Sicherheitsarchitektur muss es deshalb Ziel sein, einen standardisierten, kontinuierlichen und technisch aktuellen Austausch für relevante Cyberbedrohungsinformationen zu schaffen – auch für privatwirtschaftliche Akteure außerhalb des unmittelbaren Bundesumfelds.

4. **Technologische Entwicklungen strategisch berücksichtigen**
   Der Nationale Sicherheitsrat sollte technologische Entwicklungen mit sicherheitsrelevanter Wirkung systematisch in seine strategische Vorausschau einbeziehen. Sicherheitspolitische Entscheidungsprozesse müssen langfristige technologische Trends berücksichtigen, um Risiken frühzeitig zu erkennen und strategische Handlungsfähigkeit zu sichern. Dafür ist der kontinuierliche Zugang zu technologischem Wissen aus der Wissenschaft, aus technologienahen Stellen in den Sicherheitsbehörden, der Bundeswehr und den Bundesministerien sowie aus der Privatwirtschaft unerlässlich.

Die genannten Anforderungen zeigen, welches Potenzial ein schlagkräftig aufgestellter Nationaler Sicherheitsrat für eine moderne, integrierte Sicherheitspolitik entfalten könnte. Derzeit jedoch bleibt die praktische Umsetzung weit hinter diesem Anspruch zurück. Weder verfügt das Gremium aktuell über eine eigenständige Organisationseinheit noch über ausreichende personelle Ressourcen. Die Aufgaben werden derzeit lediglich nebenamtlich von Mitarbeitenden des Bundeskanzleramts wahrgenommen; eine institutionell verankerte Funktion eines Nationalen Sicherheitsberaters fehlt bislang vollständig. Damit droht der Nationale Sicherheitsrat auf absehbare Zeit strukturell unterdimensioniert zu bleiben – und seinem eigenen Anspruch als strategisches Koordinierungsgremium nicht gerecht zu werden. Um die sicherheitspolitischen Herausforderungen unserer Zeit wirksam zu adressieren, bedarf es nun eines entschlossenen politischen Signals: Der Nationale Sicherheitsrat muss als zentrales Element einer integrierten Sicherheitsarchitektur mit klaren Zuständigkeiten, personeller Schlagkraft und organisatorischer Eigenständigkeit ausgestattet werden.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Bereichsleiter Sicherheitspolitik
T +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik