WIRTSCHAFTSRAT
Deutschland

„Wir müssen nur wollen – mit Mut, Tempo und Führung zur Cybernation“

Positionspapier
der Bundesfachkommission
Cybersicherheit des Wirtschaftsrates

Die Stimme der Sozialen Marktwirtschaft

.

Einleitung

Deutschland steht am Scheideweg. Die sichere und nachhaltige digitale Transformation ist längst keine Zukunftsvision mehr, sie ist Realität. Doch unsere Strukturen, Strategien, unser Prozessverständnis und unser Bildungssystem sind in vielen Teilen noch analog geblieben. Wenn wir das Ziel ernst nehmen, zu einer Cybernation zu werden, dann müssen wir jetzt die Weichen stellen – ambitioniert, mutig und mit einer gemeinsamen Vision, die über Legislaturperioden hinaus Bestand hat.

Der Wirtschaftsrat der CDU e.V. vertritt über 12.000 Unternehmerinnen und Unternehmer. In der Bundesfachkommission Cybersicherheit bündeln mehr als 240 Mitgliedsunternehmen und Verbände ihre Expertise – von Technologie- und Markführern über KRITIS-Betreiber bis hin zu spezialisierten Mittelständlern.

Wir bringen alle relevanten Akteure an einen Tisch, um eine gemeinsame Vision zu schaffen – und in konkrete Strategien, Ziele und Maßnahmen zu übersetzen.

Denn eines ist klar: **Die bisherigen Ansätze reichen nicht.** Silos, Teilstrategien und unkoordinierte Einzelmaßnahmen verhindern den großen Wurf. Wenn wir so weitermachen, induzieren wir das Scheitern von Anfang an.

Wir müssen den Mut haben, **ganzheitlich, konsistent und langfristig zu denken**. Und wir müssen jetzt handeln – für kurzfristige Wirkung ebenso wie für nachhaltige Weichenstellungen.

Ein Blick auf die aktuelle Lage:

- Laut Bitkom verursacht Cyberkriminalität in Deutschland jährlich einen wirtschaftlichen Schaden von rund 200 Mrd. €.
- Die Fachkräftelücke in der Cybersicherheit beläuft sich auf über 100.000 offene Stellen.
- Bestehende Initiativen wie die Nationale Cybersicherheitsstrategie, die BSI-Reform, Gaia-X sowie die Umsetzung der NIS2-Richtlinie bilden eine solide Grundlage, erfordern jedoch eine stärkere Verzahnung und klare Governance-Strukturen und reichen allein nicht aus.
- Zentrale Herausforderungen bleiben die Zersplitterung zwischen Bund und Ländern, falsch gelebtes Ressortdenken, fehlende klare Zuständigkeiten sowie eine unzureichende Investitionsquote in strategische Sicherheitstechnologien.

1. Die Prämisse: Cybersicherheit ist mehr als Schutz

Zu lange haben wir Cybersicherheit nur als Verteidigungsaufgabe oder Domäne von Technikspezialisten verstanden. Aber sie ist weit mehr:

- Sie ist Teil der Sicherheitspolitik, weil digitale Angriffe, unkontrollierte Abhängigkeiten genauso wie militärische Bedrohungen unsere Souveränität gefährden.
- Sie ist Teil der Wirtschaftspolitik, weil wirtschaftliche Stärke, Innovationskraft und Vertrauen in den Standort Deutschland die Voraussetzung sind, einen digitalen Konflikt zu bestehen.
- Und sie ist Teil der Bildungspolitik, weil wir ohne Fachkräfte, digitale Kompetenzen und Begeisterung für MINT den internationalen Wettlauf um Köpfe verlieren.

Sicherheitspolitik ist Wirtschaftspolitik. Wirtschaftspolitik ist Sicherheitspolitik. Und beides ist ohne Bildungspolitik nichts wert.

2. Vision und Mission

Unsere Vision ist klar:
Deutschland wird Cybernation.

Unsere Mission ist ambitioniert:
Bis 2035 generiert Deutschland mehr volkswirtschaftlichen Nutzen aus Cybersicherheit, als es Schaden durch Cyberangriffe erleidet.

Das heißt konkret:

- Der wirtschaftliche Schaden durch Cyberangriffe sinkt auf unter **50 Milliarden Euro**.
- Der Umsatz der deutschen Cybersicherheits-Industrie steigt auf über **50 Milliarden Euro** – ein Weltmarktanteil von 10 Prozent
- 80 Prozent der Bevölkerung verfügen über ein **Basiswissen Cybersicherheit**, das über digitale Grundkenntnisse hinausgeht (in Anlehnung an die „Digital Decade Initiative der EU)
- Der Fachkräftemangel in der Cybersicherheit ist **vollständig überwunden**.
- Der Anteil europäischer IT-Produkte in der **deutschen Verwaltung** liegt bei 25 Prozent (wo nötig durch eine **verbindliche Quote**)

Messbare Ziele sollen alle 2 Jahre evaluiert werden, um Anpassungen an technologische, wirtschaftliche und geopolitische Entwicklungen zu ermöglichen. Der Bundesrechnungshof sollte dabei frühzeitiger und stärker in den Prozess eingebunden werden, sodass seine Rolle über die reine nachgelagerte Prüfung hinausgeht.

3. Die drei Säulen unserer Strategie

3.1. Sicherheitspolitik

Deutschland braucht eine **klare und souveräne Sicherheitsarchitektur** – von der Bundesebene bis zur Zivilgesellschaft.

- **Ebenengerechte Konzentration und Bündelung** von Verantwortlichkeiten – Silodenken durch Ressort- und Bundeslanddenken wird aufgebrochen, in dem die „Beweispflicht“ umgedreht wird. Es ist zu begründen, warum eine Verantwortungsteilung sinnvoll ist, statt wie bisher umgekehrt.
- **Schaffung eines gemeinsamen Echtzeit-Lagebilds** durch **Aufbau eines Nationalen Cyber Defense Centers (NCDC),** das Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft umfasst und auch Threat Intelligence, Härtung und Incident Response bündelt – für eine durchgängige nationale Cyberverteidigungsarchitektur
- Einführung **eines Cybersecurity-Strangs** innerhalb der Wehrpflicht und Reserve, zur Ausbildung und Integration technischer Talente in nationale Cyberverteidigungsstrukturen.
- Umsetzung des **„Cyberhilfswerk“-Gedankens** für Bürgerbeteiligung
- **Partnerschaften und Kooperation** von Staat, Wirtschaft und Bundeswehr mit gemeinsamen Übungen, Stresstests und Resillienzplänen

- **Technologische Souveränität durch Aufbau eines europäisch integrierten Zero-Trust-Stacks (Deutschland-/Euro-Stack)** als Rückgrat souveräner Sicherheitsarchitekturen. Nationale und europäische Sicherheitslösungen werden verbindlich miteinander verknüpft. Technologisch offene Architekturen und Schnittstellenstandard werden gefördert, um die Integration unterschiedlicher deutscher und europäischer Sicherheitslösungen zu erleichtern und Abhängigkeiten von proprietären Systemen nachhaltig zu reduzieren.
- **Ausbau eines nationalen Sicherheitsökosystems**, das auf vertrauenswürdige Endgeräte und souveräne Cloud-Infrastrukturen setzt.

3.2. Wirtschaftspolitik

Cybersicherheit muss zu einem **Wettbewerbsvorteil für Deutschland** werden.

- **Staat als Ankerkunde** für deutsche/europäische Anbieter
- **Förderung**, die nicht nur auf Forschung, sondern auch auf den Markteintritt abzielt und so den Fokus auf marktfertigen Innovationen legt.
- **Aufbau von nationalen Champions** in Cloud, KI, Security und Quantencomputing
- Erreichung von **Weltmarktführer-Position im** Quantencomputing und in spezialisierten KI-Systemen, um dauerhafte Defizite in anderen Bereichen auszugleichen
- Neustart der Exportinitiative und Imagekampagne „**Cybersecurity – Made in Germany**“
- **Cyber Capacity Building** mit dem wirtschaftlichen Ziel der Förderung nationaler Anbieter verbinden
- **Standardisierte Sicherheitszertifizierung** für Mittelstand und KMU und Einführung eines **Sicherheitslabels Deutschland/EU** um Marktzugang zu KRITIS und Verwaltung zu erleichtern
- Schaffung einer nationalen Beschaffungsplattform für zertifizierte Anbieter und Förderung durch Public Procurement for Innovation (PPI)
- **Führungsrolle in internationalen Standardisierungsgremien** für Cybersicherheit, KI und weiteren Schlüsseltechnologien durch Europa übernehmen
- Anpassung von **Venture-Capital- und Abschreibungsregeln**
- Aufbau eines **PPP-Cyberfonds** mit dem Ziel von 1 Mrd. € Seed-Finanzierung – getragen von Industrie und institutionellen Investoren mit Unterstützung durch den Bund – zur gezielten Förderung von Forschung, Innovation und Start-ups
- **Cybersicherheit als ESG-Kriterium** in der Unternehmensbewertung und öffentlichen Beschaffung verankern.

3.3 Bildungspolitik

Ohne Bildung kein Fortschritt. Ohne Fachkräfte keine Sicherheit.

- **Verbindlicher Informatikunterricht** in allen Bundesländern inkl. eines Pflichtmoduls „Cybersicherheit & Digitale Resilienz“ und Integration der Themen Cybersicherheit und Desinformation in die politische Bildung
- Initiierung einer nationalen **Kampagne „Sicher digital leben“** zur Sensibilisierung der Bevölkerung.

- Massive **Investitionen in MINT-Ausbildung** und **Lehrkräftequalifizierung**, u.a. durch Programme zur Frühförderung von MINT-Talenten in Grund- und Mittelstufe und Aufbau eines bundesweiten Weiterbildungsprogramms für Lehrkräfte
- Solange es einen Lehrkräftemangel gibt, sollen Brückenprojekte wie „**Classroom as a Service“** in Kooperation von Wirtschaft, Schulen und Zivilgesellschaft helfen, die Lücke zu schließen
- Aufbau eines neuen **Ausbildungsberufs „Fachinformatiker Cybersicherheit“ –** wie derzeit von eurobits gemeinsam mit der CISO Alliance regional gestartet.
- **Stärkung von Umschulung** und Quereinsteigerprogrammen
- **Steigerung des Frauenanteils** und frühzeitige Begeisterung von Kindern für IT und MINT („Wer sich 2040 vor staatlich gelenkten Cyberangriffen aus Russland, China & Co. schützen will, muss die heute Achtjährigen für MINT begeistern!“)
- Etablierung **staatlich anerkannter Zertifizierungsprogramme** (nach ISO 17024) sowie eines nationalen **Kompetenzregisters für Fachkräfte**
- **Bundesweite Cyber-Trainingszentren** als Kooperation von Wirtschaft, Verwaltung und Bildungseinrichtungen
- Förderung von **Medienkompetenz** und **Resilienz gegenüber Desinformation** – unter Einbindung bestehender Partner wie „Deutschland sicher im Netz“ (DsiN).

4. Roadmap und Zeitschiene

Zeitraum	Maßnahme	Ziel	KPI/Erfolgsmessung
2025–2026	Abschluss Strategiepapier	Vollständiges, konsistentes Konzept	Veröffentlichung des Papiers
2026–2028	Governance-Strukturen implementieren	Integration Bund, Länder, Wirtschaft, Zivilgesellschaft. Spezifizierung des Euro-/Deutschland-Stacks, Schaffung von Grundlagen für den ZeroTrust-Ansatz („Root-of-Trust“)	Anzahl aktiver Beteiligter, evaluierte Prozesse
2026–2030	Bildungsoffensive starten	Basiswissen Cybersicherheit für >50% Bevölkerung	Prozent Bevölkerung mit Basiswissen Cybersicherheit
2026–2030	Förderung nationaler Champions	Umsatzwachstum, Exportsteigerung	Umsatz, Marktanteile, Start-up-Zahlen
2030–2035	Vollständige Umsetzung Technologie-Strategie	Hohes Schutzniveau, Zero Trust, Euro-Stack	Sicherheitsindikatoren, Anzahl implementierter Standards
2030–2035	Human Factor-Expertenziel erreichen	Fachkräftemangel = 0	Anzahl Fachkräfte, offene Stellenquote
2035	Zielerreichung	Deutschland ist Cybernation	Finanzielle Schäden <50 Mrd., Industrieumsatz >50 Mrd., Bevölkerung 80% Basiswissen Cybersicherheit

Jährliche Fortschrittsberichte an Bundestag, Wirtschaft und Öffentlichkeit zur Transparenz und politischen Steuerbarkeit.

5. Kennzahlen (KPIs)

- **Finanzieller Schaden durch Cyberangriffe** (Mrd. EUR, lt. Bitkom-Studie)
- **Umsatz der Cybersicherheits-Industrie** (national und international)
- **Marktanteil deutscher Anbieter** (national/ global)
- **Europäischer Produktanteil in deutscher Verwaltung**
- **Fachkräftezahlen** (Cybersicherheits-Experten, Ausbildung, Umschulung)
- **Basiswissen Cybersicherheit der Bevölkerung** (in Prozent der Bevölkerung)
- **Technologie-Souveränität** (Anteil kritischer Systeme mit national/europäischer Technologie)
- **Kooperation Wirtschaft-Staat-Bundeswehr** als **Public-Private-Partnership Index** (Anzahl gemeinsamer Projekte, Übungen, Hospitationen)
- **Medienkompetenz & Resilienz der Bevölkerung** (Umfrageindikatoren, Engagement in Awareness-Programmen)
- **Operative Resilienz als Indikator** (Anzahl kritischer Sicherheitsvorfälle und Median-Reaktionszeit darauf, auch Mean Time to Respond, kurz MTTR, bezeichnet)

6. Fazit

Deutschland steht an einem Wendepunkt. Wir können die Cybernation Europas werden – oder zum digitalen Risiko. Noch ist es eine Chance. Aber sie wird nicht ewig warten. Cybersicherheit muss zur Schlüsselindustrie des 21. Jahrhunderts werden – made in Germany. #and Europe

Nicht nur als Schutzschild, sondern als Wachstumsbooster, Innovationsmotor und Garant unserer digitalen Souveränität. Aber dafür braucht es mehr als Strategiepapiere.

Es braucht politischen Willen. Es braucht Führung. Es braucht den Mut zur Tat.

Jetzt.

Wollen wir wirklich gestalten – oder wieder nur verwalten?

Die Uhr tickt.