WIRTSCHAFTSRAT
Deutschland

Wir bauen die Cybernation

Eine Strategie für eine sichere, souveräne und prosperierende Zukunft

Wir bauen die Cybernation

-

Eine Strategie für eine sichere, souveräne und prosperierende Zukunft

Vorwort

Vor einem Jahr hat der Wirtschaftsrat mit der Konferenz „Wir bauen die Cybernation“ eine Initiative angestoßen, um den Weg dorthin aufzuzeigen.

Heute legen wir ein in seiner Herangehensweise einzigartiges Werk vor. Wir haben die Themen Sicherheits-, Wirtschafts- und Bildungspolitik integral betrachtet und mit vielen Experten aus jeder dieser Perspektiven eine zukunftsweisende Strategie mit konkreten Vorschlägen und Handlungsempfehlungen erarbeitet.

Gehen wir diese Themen wie bisher isoliert an, werden wir scheitern. Betrachten wir sie zusammen, haben wir sehr gute Erfolgsaussichten. Dies bedingt, dass wir Cybersicherheit nicht mehr als Risiko betrachten, sondern als Chance.

Wir haben in Deutschland keine seltenen Erden, aber wir haben seltene Fähigkeiten. Und wir haben Talente. Wenn wir diese fördern und ihnen auf staatlicher und wirtschaftlicher Ebene einen Rahmen bieten, diese optimal einzusetzen, so werden wir auch in Zukunft nicht nur in Sicherheit, sondern auch souverän in Wohlstand leben können.

Wir hoffen, dass dieses Buch einen Beitrag dazu leisten kann.

Wolfgang Steiger
Generalsekretär
Wirtschaftsrat der CDU e.V.

Prof. Timo Kob
Vorsitzender BFK Cybersicherheit
Aufsichtsratsvorsitzender HiSolutions AG

Inhaltsverzeichnis

Unser strategischer Ansatz 11

Unsere Empfehlungen 22

A) Staatliche Sicherheitsarchitektur 23

1. Entwicklung des Nationalen Sicherheitsrats zu einem übergreifenden Sicherheitsgremium 23
2. Sicherstellung einer Führungsrolle bei Schwachstellenerkennung durch KI 25
3. Schaffung eines Nationalen Cyber Defense Centers (NCDC) 27
4. Entwicklung einer klaren und messbaren Cybersicherheitsstrategie des Bundes 29
5. Modernisierung des Sicherheitsüberprüfungsrechts und des Geheimschutzes 30
6. Konsolidierung der staatlichen Sicherheitsarchitektur .. 34
7. Definition einer klaren strategischen Ausrichtung des BSI 36
8. Konsolidierung staatlicher Forschungsinstitutionen 37
9. Strategie als dauerhafter Prozess: externe Partner verbindlich einbinden 39
10. Schaffung eines Lagebilds der Cyberkompetenzen und -Ressourcen 40

11. Verbindliche Verankerung gemeinsamer Übungen und Sektoren-SPOCs 41
12. Schaffung von IT-Sicherheitsmindeststandards für Parteien und Fraktionen 43
13. Wirksamkeit und Verbindlichkeit der Bundesrechnungshof-Berichte sichern..... 44
14. Einrichtung eines Cyber Safety Review Boards 45
15. Vertrauensbildende Maßnahmen zwischen Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft 47
16. Offensivere Kommunikation staatlicher Fähigkeiten 49
17. Konsequente Ausnutzung des Sanktionsrahmens 50
18. Integration eines Cybersecurity-Strangs in Wehrpflicht und Reserve..... 51

B) Schutz von Ländern und Kommunen 53

19. Klare Verantwortlichkeiten und Führungsstrukturen auf Landes- und Kommunalebene..... 53
20. Etablierung einer verbindlichen Bund-Länder-Kommunen-Governance für Cybersicherheit 55
21. Etablierung verbindlicher Mindeststandards für Länder und Kommunen 57
22. Schaffung sicherer kommunaler Datenräume und von Interoperabilität 59
23. Konsolidierung des IT-Betriebs der Kommunen 60

24. Etablierung zentral verfügbarer Sicherheitsdienste für Kommunen 61
25. Finanzierung von Cybersicherheit als Pflichtaufgabe 62
26. Strategische Neudefinition der Rolle der IT-Dienstleister der Länder 63
27. Schaffung einheitlicher Sicherheitsanforderungen an kommunale IT-Dienstleister 64
28. Qualifizierung, Personalbindung und Entlastung der Verwaltung 65
29. Definition klarer Schnittstellen zu Polizei-, Verfassungs- und Katastrophenschutzstrukturen 67
30. Festlegung klarer Melde-, Unterstützungs- und Eingriffsmechanismen im Cybervorfall 68
31. Institutionalisierung eines föderalen Krisenmanagements für Cyberlagen 69
32. Aufbau einer föderalen Lern- und Wissensplattform für kommunale Cybersicherheit 70

C) Cybersicherheit als Wirtschaftspolitik 71

33. Staat als strategischer Ankerkunde für deutsche und europäische Anbieter 71
34. Stärkung einer Förderpolitik, die den tatsächlichen Markteintritt unterstützt 73
35. Aufbau einer Nationalen Beschaffungsplattform für zertifizierte Anbieter und konsequentes PPI 75

36. Neuausrichtung und Erweiterung einer Exportinitiative und Imagekampagne „Cybersecurity - Made in Germany" 77
37. Aufbau nationaler Champions in Cloud, KI, Security und Quantencomputing 78
38. Erreichung einer Weltmarktführerposition in Post-Quantum-Kryptographie und spezialisierten KI-Systemen 80
39. Stärkere Berücksichtigung von Industriepolitik beim Cyber Capacity Building 82
40. Etablierung praxisnaher Zertifizierungspfade und Schaffung eines Sicherheitslabels GER × EU 83
41. Übernahme von Führungsrollen in internationalen Standardisierungsgremien 85
42. Verbesserung der Kapitalverfügbarkeit für Cybersecurity-Unternehmen 87
43. Aufbau eines PPP-Cyberfonds 88

D) Digitale Souveränität 90

44. Schaffung eines verbindlichen Prüfschemas für kritische, digitale Abhängigkeiten 91
45. Definition und Umsetzung verbindlicher Resilienz-Baselines 93
46. Konsequente Priorisierung strategischer Kontrollpunkte 94

47. Verankerung des Leitprinzips datenzentrierter Sicherheitsarchitektur 96
48. Aufbau eines europäisch integrierten Zero-Trust-Stacks zur Erreichung technologischer Souveränität 98
49. Aufbau einer Nationalen Cyber-Architekturplattform mit Service-Katalog und Marketplace 100

E) Bildung von der Kita bis zur Seniorenresidenz 104

50. Massive Investitionen in MINT-Ausbildung und Lehrkräftequalifizierung 106
51. Einführung von Informatik als durchgängiges Pflichtfach in allen Bundesländern 108
52. Verbindliche Verankerung von Cybersicherheit im Informatik-Lehrplan 110
53. Aufbau eines Quereinsteigerprogramms für Informatiklehrer 112
54. Einrichtung eines Ausbildungsberufs „Fachinformatiker(in) Cybersicherheit“ 114
55. Steigerung des Anteils weiblicher Fachkräfte 116
56. Ermöglichung und Förderung von ehrenamtlichem Engagement aus Wirtschaft und Gesellschaft 120
57. Erstellung einer flächendeckenden, zielgruppen-spezifischen und koordinierten Awareness-Kampagne 122

F) Prinzipien für einen nachhaltigen Erfolg..... 125

58. Entwicklung eines Cybernation-Prinzipienkatalogs..... 126

Schlussbetrachtung..... 128

Literaturverzeichnis 130

Unser strategischer Ansatz

Fast schon wie die Aussage, dass der Mittelstand das wirtschaftliche Rückgrat unseres Landes ist, gehört auch die Aussage, dass wir kein Erkenntnis- sondern „nur“ ein Umsetzungsproblem haben, seit Jahrzehnten zum festen Inventar deutscher Politikdebatten. Aber ist dem wirklich so? Kann es sein, dass wir zwar die Erkenntnis haben, was falsch läuft, uns aber die Erkenntnis fehlt, wie wir das Umsetzungsproblem lösen?

Vorschläge, wie die Defizite unserer Gesellschaft und Volkswirtschaft, die sich in den letzten Jahren und Jahrzehnten aufgestaut haben, behoben werden können, gibt es viele. Seien es die Ergebnisse der „Initiative für einen handlungsfähigen Staat“, seien es die „100 Vorschläge für den Neustaat“ sowie viele andere kluge und produktive Papiere.

Das vorliegende Papier wird viele Handlungsempfehlungen ergänzen. Unser thematischer Fokus ist deutlich kleiner und spezifischer als beispielsweise jener der obengenannten Beiträge. Dies ermöglicht uns aber gleichzeitig, „vollständiger“ vorzugehen, da wir für dieses abgegrenzte Thema leichter ein komplettes Bild aufzeigen können. Wir sind fest davon überzeugt, dass ein Teil der Schwierigkeiten bei der Durchsetzung von notwendigen Reformen darin liegt, dass zu schnell in operative Maßnahmen abgetaucht und der strategische Rahmen vergessen wird. Wir brauchen eine Vision und Mission, ein positives Narrativ, um alle Seiten

mitzunehmen und Veränderungen zumutbar zu machen. Das Beheben eines erkannten Fehlers ist kein Mehrwert, das Schaffen einer besseren Lösung ist es.

Und dieses „Bessere Neue“ muss diskutiert, ja ausgehandelt werden. Dies gilt im Großen wie im Kleinen: wofür will Deutschland in 20 Jahren stehen, was will es sein? Sind wir noch die Autobauer, Maschinebauer und Apotheker der Welt? Und wenn Nein, was dann? Hinter welcher Vision oder bildlich gesprochen welchem Banner wollen wir uns versammeln? Wir glauben fest, dass dieses positive, aktive „Für etwas arbeiten“ ganz andere Energien freisetzen kann und wird, als ein passives „Wir müssen Fehler beheben“, wie wir es derzeit gerade sehen.

Gegen all die Verkrustungen, Versäumnisse und Resignationen wollen wir ein positives Narrativ setzen, überspitzt gesagt ein „Project Moonshot“, so wie Kennedy 1962 den Weg der USA zum Mond skizzierte.

Und seien wir ehrlich: nichts weniger als einen solchen „Moonshot“ brauchen wir, um uns im gesamten Thema Digitalisierung zeitnah in eine Position zu bringen, die uns erlaubt, unseren Status als eine führende Industrienation zu behalten, respektive im Digitalen Raum zurückzugewinnen. Und ein toller Slogan reicht dafür nicht aus, aus dem Slogan muss eine klare Vision und Mission werden. Aus der Mission muss ein klarer strategischer Handlungsauftrag werden, mit konkreten Zielen, Teilzielen und Maßnahmen, mit konkreten KPIs und Fristen.

Und mit einem Blick, der weder die Scheuklappen „Föderalismus“, „Ressortunabhängigkeit“ noch „Legislaturperiode“ kennt. Und wenn wir dies stringent von unserem Ziel aus ableiten, werden wir feststellen, wie breit und vielfältig die Schrauben verteilt sind, an denen wir justieren müssen, aber positiv ausgedrückt eben auch können, um unser Ziel zu erreichen.

Für unser Land können wir uns als Bundesfachkommission Cybersicherheit dies wünschen, aber nicht leisten. Aber hier kommt der Slogan „Cybernation“ ins Spiel. Was wir für Deutschland nicht können, können wir für die Cybernation.

Und wenn uns hier ein Fortschritt gelingt, so ist das eben auch wieder ein Erkenntnisgewinn, wie wir unser Umsetzungsproblem beheben. Mit positivem Narrativ als wirkliche Strategie, mit Blick über die Tellerränder, mit einer breiten Koalition von motivierten Mitstreitern und klaren Zielen sowie verbindlichen Fristen.

Und wenn wir es für die Cybernation können, so motiviert es vielleicht andere, es für weitere Teile unserer „Future Nation“ zu tun.

Doch was bedeutet dieser Anspruch und Ansatz in der Praxis? Um zu einem positiven Ziel und Erzählung zu kommen, brauchen wir einen Perspektivwechsel, genauer gesagt: ein neues Mindset. Cybersicherheit ist bei uns ein Angstthema, bei dem es darum geht, den Schaden zu reduzieren. Wer spielt gerne Spiele, bei denen es

nicht darum geht, zu gewinnen, sondern nur darum, weniger zu verlieren?

Wir wollen mit Cybersicherheit gewinnen und wir glauben, dass allein dieser „change of the game“ bei konsequenter Anwendung der „Gamechanger“ ist.

Unsere Vision heißt also:

„Wir wollen eine der führenden Nationen in allen Aspekten der Cybersicherheit sein und unsere Volkswirtschaft verdient mehr Geld mit dem Thema Cybersicherheit, als sie Schäden erleidet“.

Unsere daraus abgeleitete Mission ist also:

„Wir sorgen dafür, dass die Schadenshöhe durch Cybersicherheitsvorfälle massiv reduziert und parallel die Umsätze der deutschen Cybersicherheits-Industrie so gesteigert werden, dass sie die Schäden übertreffen.“

Konkret in Zahlen ausgedrückt:

Bis zum Jahre 2035 sinkt die Schadenshöhe durch Cyberattacken gemäß BITKOM-Studie von derzeit gut 200 Milliarden Euro auf unter 50 Milliarden Euro. Gleichzeitig steigt der Umsatz der deutschen Cybersicherheits-Industrie auf über 50 Milliarden Euro des Basiswertes.

Um dies ins Verhältnis zum Status quo zu setzen:

Aktuelle Schätzungen des BITKOM gehen von einem wirtschaftlichen Umsatzvolumen der deutschen Cybersecurity-Industrie von 11 Milliarden Euro im Jahre 2025 aus (davon 6 Milliarden Soft- und Hardware).

Weltweit wird in der gleichen Studie von einem Markt in Höhe von 212 Milliarden Euro ausgegangen. Der deutsche Weltmarktanteil beträgt also 5,3 %.

Gehen wir von einem durchschnittlichen Wachstum von 10 % aus, so besitzt der Weltmarkt 2035 ein Volumen von gut 570 Milliarden Euro und der deutsche Umsatz würde rund 28 Milliarden betragen. Unser Ziel ist es übertragen, den Weltmarktanteil Deutschlands von gut 5 % auf rund 10 % zu steigern. Dies ist sicher ambitioniert, aber wir glauben, dass dies für die drittgrößte Volkswirtschaft ein angemessenes Ziel ist. Ist es zu ambitioniert, wenn wir als Land zumindest einen doppelt so großen Weltmarktanteil haben wollen, wie das größte Privatunternehmen heute?

Umgekehrt ist aber auch offensichtlich, dass dies nur machbar ist, wenn das Thema Cybersicherheit ganz anders betrachtet wird, als es bisher größtenteils der Fall ist. Aus einem sicherheitspolitischen Thema - in all seinen Facetten - muss viel stärker gleichsam ein wirtschafts-, industrie- und auch forschungspolitisches Thema werden.

Wachsende technologische Abhängigkeiten von außereuropäischen Anbietern, sprich mangelnde digitale Souveränität sowie strukturelle Defizite bei Skalierung, Finanzierung und Marktzugang kennzeichnen die wirtschaftliche Dimension dieses Problems.

Digitale Souveränität ist zu einem Leitbegriff der Debatte geworden – zu oft bleibt er abstrakt oder wird als Marketinggag pervertiert. Mal erscheint sie als Wunsch nach vollständiger technologischer Unabhängigkeit, mal als industriepolitische Chiffre ohne operative Konsequenz. Beides greift zu kurz. Für eine vernetzte Volkswirtschaft wie Deutschland ist weder vollständige Autarkie realistisch noch jede Form technologischer Abhängigkeit problematisch. Dabei ist ausdrücklich zwischen strategischen Abhängigkeiten und normaler globaler Arbeitsteilung zu unterscheiden. Nicht jede Nutzung außereuropäischer Technologien stellt per se ein sicherheitspolitisches Risiko dar. Entscheidend ist vielmehr, ob Abhängigkeiten kritische Steuerungsfähigkeit in Krisen oder unter politischem Druck einschränken. Globale Arbeitsteilung, internationale Lieferketten und technologische Kooperation sind zentrale Voraussetzungen für Innovation, Wohlstand und Wettbewerbsfähigkeit. Entscheidend ist daher nicht die pauschale Vermeidung jeglicher Abhängigkeiten, sondern die Fähigkeit, strategisch kritische Abhängigkeiten zu erkennen, zu bewerten und aktiv zu steuern.

Souverän ist, wer kritische digitale Funktionen auch unter Druck verlässlich steuern, schützen, aufrechterhalten und weiterentwickeln kann. Souverän ist auch, wer auf einem nicht

einseitig dominierten Markt echte Wahlfreiheit besitzt. Der Maßstab ist daher Handlungsfähigkeit in Interdependenz: die Fähigkeit, Abhängigkeiten nicht zu leugnen, sondern sie so zu verstehen, zu härten und zu steuern, dass Deutschland und Europa auch unter Stress entscheiden und handeln können.

Diese Form von Souveränität bedarf gleichsam entsprechender Fachkräfte.

Und wenn wir dies weiterdenken und uns ansehen, wie groß unser Problem heute ist, allein für die sicherheitspolitische Seite der Abwehr von Angriffen genügend Fachpersonal zu gewinnen, erkennen wir unser Problem. Wie groß wird diese Lücke erst, wenn wir gleichzeitig souveräner und wirtschaftlich erfolgreicher, also hier konkret im Cybersecurity-Sektor unseren Weltmarktanteil verdoppeln wollen?

Es ist also offensichtlich, dass wir nicht nur massive Anstrengungen und Änderungen in Sicherheits- und Wirtschaftspolitik benötigen, sondern dies in mindestens gleichem Maße auch in unserer Bildungspolitik.

Wir haben in Deutschland kaum seltene Erden, aber als traditionelles „Ingenieursland“ seltene Fähigkeiten. Umso wichtiger ist es, dass unsere Fachkräfte nicht zu Raritäten werden.

Wir müssen viel mehr Fachkräfte ausbilden. Dies wird uns nur gelingen, wenn wir rigoros Lehrpläne modernisieren und dem

Thema Digitalisierung in seiner ganzen Breite (und nicht nur diesem) den Platz einräumen, den es in einer modernen Gesellschaft verdient.

Kristina Kallas, die Bildungs- und Forschungsministerin Estlands wird im Tagesspiegel wie folgt zitiert: „Die wirtschaftliche Wettbewerbsfähigkeit Estlands hängt davon ab, wie gut wir junge Menschen auf das Zeitalter der Künstlichen Intelligenz vorbereiten."

Dies gilt für Deutschland umso mehr, da wir dies bereits für das gesamte Thema der Digitalisierung verpasst haben. Und es geht bei Thema Cybersicherheit eben nicht nur um wirtschaftliche Wettbewerbsfähigkeit, sondern auch um die gesamte Verteidigungsfähigkeit.

Aber es geht auch nicht nur um unsere Kinder, sondern um die gesamte Bevölkerung. Die Gleichung ist ganz einfach: je besser unsere Bevölkerung in der Gesamtheit hier Kompetenzen aufbaut, sich selbst zu schützen - Stichwort Herdenimmunität - desto weniger Fachkräfte brauchen wir, um sie zu schützen. Und je effizienter wir unseren Schutz organisieren, desto weniger Fachkräfte müssen wir hier binden und können diese für die Erreichung unserer wirtschaftlichen Ziele nutzen.

Und so schließt sich der Kreis:

Sicherheitspolitik ist Wirtschaftspolitik ist Bildungspolitik ist Sicherheitspolitik!

Ist dies akzeptiert, so kommen wir zu den detaillierteren Handlungs- und Problemfeldern, die wir hier skizzieren und in den folgenden Kapiteln in eine konkrete Strategie gießen.

Die oben postulierte Effizienz sowie die erforderliche Effektivität in unseren Verteidigungsanstrengungen sind mit der heutigen Ausprägung unserer Sicherheitsarchitektur und der heutigen Interpretation des Föderalismus nicht erreichbar. Die Sicherheitsarchitektur Deutschlands im Cyberbereich ist heute fragmentiert, unzureichend koordiniert und strukturell nicht auf die Bedrohungslage ausgerichtet, der wir gegenüberstehen. Isolierte Zentren – als Beispiele seien das Gemeinsame Terrorismusabwehrzentrum (GTAZ) das Gemeinsame Extremismus- und Terrorismusabwehrzentrum (GETZ) oder das Nationale Cyber-Abwehrzentrum (NCAZ) genannt - arbeiten weitgehend nebeneinander, ohne in ein gemeinsames, ressortübergreifendes Lagebild eingebettet zu sein. Zuständigkeiten bleiben in vielen Bereichen ungeklärt. Silodenken nach Ressort- und Bundeslandlogik verhindert die notwendige Konzentration von Verantwortung. Eine kohärente nationale Strategie fehlt ebenso wie die institutionellen Voraussetzungen, um sie dauerhaft umzusetzen.

Gleichzeitig hat sich die geopolitische Lage grundlegend verändert. Der völkerrechtswidrige Angriff auf die Ukraine, die wachsende strategische Rivalität zwischen den USA und China sowie die tiefgreifenden Verschiebungen in der globalen Technologieordnung haben aus Cybersicherheit endgültig eine geopolitische Schlüsselfrage gemacht. Deutschland und Europa befinden sich in einer asymmetrischen Wettbewerbssituation: Während die USA und China Cyber-, KI- und Plattformtechnologien massiv skalieren und interdisziplinär vernetzen, verbleibt Europa in fragmentierten, forschungszentrierten Ansätzen mit begrenzter Marktdurchdringung. Der Draghi-Report (2024) diagnostiziert für Europa grundlegende Defizite bei Innovation, Investition und Skalierung. Im Cyberbereich sind diese Defizite besonders kritisch, weil technologische Abhängigkeiten hier unmittelbar sicherheitspolitische Risiken erzeugen können.

Diese Handlungsfähigkeit entscheidet sich nicht überall zugleich. Sie verdichtet sich an wenigen strategischen Kontrollpunkten, an denen digitale Steuerungsfähigkeit tatsächlich gewonnen oder verloren wird: Endpunkte, Identitäten, Datenräume sowie zentrale Steuerungs- und Betriebsebenen. Wer diese Kontrollpunkte beherrscht, kann digitale Systeme gestalten. Wer sie verliert, verliert nicht nur Sicherheit, sondern operative und politische Handlungsfähigkeit. Die Konzentration auf diese Kontrollpunkte dient zugleich dazu, politische Aufmerksamkeit, regulatorische Maßnahmen und finanzielle Ressourcen auf jene Bereiche zu fokussieren, in denen sie die größte sicherheitspolitische und wirtschaftliche Wirkung entfalten.

Ein klassischer Maßnahmenkatalog allein reicht jedoch nicht aus. Künstliche Intelligenz, Automatisierung und neue Angriffsformen können bestehende Annahmen innerhalb weniger Monate verändern. Die Cybernation Deutschland braucht deshalb neben konkreten Maßnahmen auch einen prinzipiengeleiteten Ansatz: Handlungsfähigkeit vor Autarkie, Kontrolle an strategischen Kontrollpunkten, Sicherheit als Ermöglicher von Zusammenarbeit, aktive Steuerung kritischer Abhängigkeiten sowie gemeinsame Standards bei föderaler Umsetzung.

Unsere hier vorliegende Strategie beinhaltet nicht nur Vision, Mission, Ziele und Maßnahmen, sondern auch einen prinzipiengeleiteten Rahmen zur Sicherung eines nachhaltigen Erfolges.

Per se besitzt dieses Papier keinen Anspruch auf Vollständigkeit, sondern versteht sich als dynamisches Modell. Die Vorstellung ist gleichzeitig der Startschuss in die nächste Runde.

Auf den folgenden Seiten fassen wir unsere 58 Handlungsempfehlungen in 6 Bereichen zusammen:

A) Staatliche Sicherheitsarchitektur
B) Schutz von Ländern und Kommunen
C) Cybersicherheit als Wirtschaftspolitik
D) Digitale Souveränität
E) Bildung von der Kita bis zur Seniorenresidenz
F) Prinzipien für einen nachhaltigen Erfolg

Unsere Empfehlungen

A) Staatliche Sicherheitsarchitektur

1. Entwicklung des Nationalen Sicherheitsrats zu einem übergreifenden Sicherheitsgremium

Sicherheitspolitisch handlungsfähig zu sein bedeutet, alle relevanten Bedrohungslagen ressortübergreifend zu erfassen und zu bewerten. Der Nationale Sicherheitsrat ist dafür der geeignete institutionelle Rahmen. Er muss jedoch grundlegend gestärkt werden.

Wir empfehlen:

- Integration der bestehenden Zentren (NCAZ, GTAZ, GETZ und weitere) in die Struktur des Nationalen Sicherheitsrates wird durch klare Zielkennzahlen gesteuert. Bis 2027 sollen 100 % der relevanten Einheiten organisatorisch eingebunden sein; bis 2030 sollen redundante Parallelstrukturen vollständig abgebaut sein.
- Die Fähigkeit zur ressortübergreifenden Lagebilderstellung - Time to Common Operating Picture (TCOP) - wird als zentrale Steuerungsgröße definiert. Ziel ist die Erreichung eines Wertes von unter 24 Stunden bis spätestens 2028,

um im Krisenfall schnelle Handlungsfähigkeit zu garantieren. Längerfristiges Ziel ist die Erreichung ein TCOP=0, sprich die jederzeitige Verfügbarkeit eines ressortübergreifenden Lagebildes in Echtzeit.

- Qualität und Kohärenz des Lagebilds werden halbjährlich evaluiert; Fortschritte bei Integration und Governance werden quartalsweise gemessen und berichtet.

2. Sicherstellung einer Führungsrolle bei Schwachstellenerkennung durch KI

Die aktuellen Tendenzen und Fortschritte bei der Schwachstellenerkennung durch Künstliche Intelligenz beinhalten eine dramatische neue Gefahr für Souveränität und nationale Sicherheit. Wir müssen sicherstellen, dass Deutschland und Europa im Bereich der Schwachstellenerkennung durch KI mit den anderen Großmächten mithalten kann. Wenn wir nicht Zugang zu den aktuellen Modellen haben - oder noch besser: selbst welche entwickeln - werden wir in einen ungeahnten Grad von Erpressbarkeit geraten. Souveränität und nationale Sicherheit sind ohne diese nicht denkbar, die Asymmetrie höchstens vergleichbar mit der zwischen Nuklearmächten und konventionell bewaffneten Staaten. Dies ist also keine rein wissenschaftlich-technische Frage, sondern bedingt ein enges Zusammenspiel zwischen Nationalen Sicherheitsrat, den technischen Teilen der Sicherheitsbehörden und dem Forschungsökosystem. Wir unterstützen die Forderung des BSI nach Etablierung einer zentralen Anlaufstelle für Nutzung und Bewertung von Frontier-KI-Modellen zur Schwachstellen-analyse als solches Scharnier.

Wir empfehlen:

- Zugang zu den aktuellen KI-Modellen zur Schwachstellen-findung ausbauen und quantitativ messbar machen.

- Entwicklung gleichwertiger Systeme aus Europa und für Europa. Hierzu werden Sicherheitsbehörden, Forschungsinstitutionen und Unternehmen in einem europäischen Innovationsökosystem zusammengeführt, um eigene KI-Systeme zur Schwachstellenerkennung für Europa zu entwickeln und dauerhaft technologisch wettbewerbsfähig zu halten.
- Eine weitere Option ist die Gründung einer PPP bspw. durch das BSI und/oder das Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) mit Bedarfsträgern im Staat wie etwa dem Bundesministerium der Verteidigung oder dem Bundesministerium des Innern etc. und relevanten Unternehmen
- Optimierung des Zusammenspiels zwischen Sicherheitsforschern, politischen Entscheidungsträgern, Behörden und Unternehmen, um Schwachstellenfindung, politisch-strategische Bewertung und operative Schwachstellenbehebung bis in die gesamte Wirtschaft zu ermöglichen.
- Für den Einsatz KI-gestützter Systeme zur Schwachstellenerkennung sind klare Governance-Strukturen zu schaffen. Dazu gehören rechtliche Leitplanken, transparente Verantwortlichkeiten, Auditierbarkeit der Systeme sowie Vorkehrungen gegen Missbrauch – insbesondere bei staatlicher Nutzung. Die technologische Leistungsfähigkeit muss stets durch ethische und rechtliche Kontrollmechanismen flankiert werden.

3. Schaffung eines Nationalen Cyber Defense Centers (NCDC)

Ein einheitliches Lagebild im Cyberbereich existiert bislang nicht. Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft agieren weitgehend unkoordiniert. Das muss sich ändern. Die bisher zur Verfügung stehenden Informationen zum geplanten Cyberdome scheinen in die Richtung zu deuten, dass ein solcher Ansatz geplant ist, hier bedarf es aber weiterer Konkretisierungen.

Wir empfehlen:

- Für das NCDC werden operative Leistungskennzahlen als föderal aggregierte Steuerungsgrößen definiert: Mean Time to Detect (MTTD) und Mean Time to Respond/Recover (MTTR) beziehen sich auf meldepflichtige bzw. lagebildrelevante Vorfälle, die über NIS2/BSIG, DORA und sektorale Meldewege erfasst werden. Das NCDC detektiert Vorfälle nicht zentral selbst, sondern standardisiert Erfassung, Lagebild, Koordination und Auswertung. Die strategische Rückbindung erfolgt an den Nationalen Sicherheitsrat.
- Bis 2028 sollen MTTD und MTTR gegenüber der 2026 zu erhebenden Baseline um mindestens 30 % sinken. Die 30 %-Zielgröße ist als politischer Mindestambitionswert plausibilisiert: IBM/Ponemon zeigen 2025, dass breite Security-AI- und Automatisierungsnutzung den Breach

Lifecycle im Durchschnitt um 80 Tage verkürzt; 2024 wurden bei intensiver Security-AI-Nutzung im Durchschnitt nahezu 100 Tage schnellere Identifikation und Eindämmung berichtet. Ein 30 %-Ziel ist ein belastbarer, benchmarkfähiger Zielkorridor für Deutschland, sofern Messdefinition und Baseline einheitlich festgelegt werden.

- Bis 2028 werden alle relevanten staatlichen Akteure vollständig integriert; bis 2030 erfolgt die strukturierte Anbindung von mindestens 70 % der KRITIS-Betreiber an das nationale Lagebild.
- Leistungsfähigkeit des Threat-Intelligence-Systems wird monatlich gemessen (u. a. Anzahl verwertbarer Lageberichte, Reaktionszeiten) und jährlich umfassend evaluiert.
- Die Ausgestaltung des NCDC berücksichtigt von Beginn an die föderale Struktur Deutschlands. Länder werden über verbindliche Governance-Mechanismen, gemeinsame Lagebilder und abgestimmte Zuständigkeiten eingebunden, um Doppelstrukturen zu vermeiden und die politische wie administrative Akzeptanz dauerhaft sicherzustellen.

4. Entwicklung einer klaren und messbaren Cybersicherheitsstrategie des Bundes

Bisherige Strategiedokumente des Bundes bleiben abstrakt. Statt konkreter Ziele, Zeitrahmen und Maßnahmen enthalten sie vor allem Absichtserklärungen. Das reicht nicht aus.

Wir empfehlen:

- Cybersicherheitsstrategie wird vollständig KPI-basiert ausgestaltet.
- Bis 2027 enthalten 100 % der Maßnahmen konkrete Zielwerte, Zeitrahmen und Budgetangaben.
- Bis 2028 sollen mindestens 75 % der definierten Maßnahmen in Umsetzung sein; bis 2030 wird ein Zielerreichungsgrad von mindestens 90 % angestrebt.
- Fortschritte werden halbjährlich gemessen; ein jährlicher Strategiereview passt Ziele, Kennzahlen und Maßnahmen systematisch an.

5. Modernisierung des Sicherheitsüberprüfungsrechts und des Geheimschutzes

Das Sicherheitsüberprüfungsgesetz (SÜG) und die bestehenden Verfahren des personellen und materiellen Geheimschutzes sind in ihrer heutigen Form nicht mehr ausreichend, um die Anforderungen moderner Sicherheitsarchitekturen zu erfüllen. Dies gilt insbesondere dort, wo Kritische Infrastrukturen, sicherheitsrelevante Unternehmen, Cybersecurity-Anbieter und digitale Schlüsselprojekte betroffen sind.

In einer Welt, in der Cybersicherheit, KI, Cloud-Infrastrukturen, Lieferketten und geopolitische Risiken immer enger miteinander verbunden sind, wird Vertrauenswürdigkeit zu einer zentralen Voraussetzung staatlicher und wirtschaftlicher Handlungsfähigkeit. Sicherheitsüberprüfungen sind deshalb nicht weniger wichtig geworden, sondern erheblich wichtiger. Gleichzeitig werden sie selbst zum Engpass, wenn Verfahren zu lange dauern, zu wenig abgestuft sind oder nicht ausreichend digital unterstützt werden.

Die heutige Lage erzeugt ein strategisches Paradox: Deutschland braucht deutlich mehr überprüfte, vertrauenswürdige Personen und Organisationen in sicherheitsrelevanten Bereichen, aber die Verfahren zur Herstellung dieser Vertrauensbasis sind zu langsam, zu analog und zu wenig skalierbar. Damit wird nicht nur Verwaltung verlangsamt. Es werden Innovation, Marktzugang, KRITIS-Sicherheit und nationale Cyberresilienz behindert.

Wir empfehlen deshalb nicht nur eine moderate Beschleunigung, sondern einen grundlegenden Technologiesprung. Innerhalb von weniger als einem Jahr sollte ein digital unterstütztes, KI-gestütztes Alternativ- oder Äquivalenzverfahren entwickelt werden, das Sicherheitsüberprüfungen in geeigneten Fällen um Größenordnungen beschleunigt. Ziel muss sein, bestimmte standardisierbare Prüf- und Vorprüfprozesse nicht um 30 Prozent, sondern perspektivisch um den Faktor 100 zu verkürzen – also von Monaten auf Tage oder Stunden, soweit dies rechtlich, fachlich und sicherheitlich vertretbar ist.

Dies bedeutet ausdrücklich nicht, Sicherheitsanforderungen abzusenken. Im Gegenteil: Moderne IT- und KI-Unterstützung kann die Qualität, Nachvollziehbarkeit und Aktualität von Prüfungen erhöhen, wenn Datenquellen besser verbunden, Risiken dynamischer bewertet und manuelle Routinetätigkeiten automatisiert werden. Entscheidend ist ein abgestuftes Modell: einfache Vertrauenswürdigkeitsprüfungen für KRITIS-nahe Tätigkeiten, vertiefte Sicherheitsüberprüfungen für besonders sensible Rollen und kontinuierliche, risikobasierte Aktualisierung dort, wo statische Einmalprüfungen nicht mehr ausreichen.

Wir empfehlen:

- Das SÜG wird durch ein modernes Geheimschutz- und Vertrauenswürdigkeitsgesetz ersetzt oder ergänzt, das abgestufte Prüfmodelle für Staat, KRITIS und sicherheitsrelevante Wirtschaft vorsieht.

- Der personelle und materielle Geheimschutz wird umfassend modernisiert, unter besonderer Berücksichtigung der Wirtschaft und der Betreiber Kritischer Infrastrukturen.
- Die durchschnittliche Dauer von Sicherheitsüberprüfungen wird als zentrale Kennzahl definiert und bis 2028 um mindestens 30 % reduziert.
- Effizienz und Akzeptanz der Verfahren werden quartalsweise anhand von Bearbeitungszeiten und jährlich durch Befragungen von Unternehmen und KRITIS-Betreibern gemessen und veröffentlicht.
- Innerhalb von zwölf Monaten wird ein digitaler, KI-gestützter Prüfpfad als Alternative oder Äquivalent zu bestehenden Verfahren entwickelt und pilotiert.
- Für 2030 ist die Zielgröße nicht nur eine 30-prozentige Beschleunigung, sondern eine radikale Verkürzung standardisierbarer Prüfprozesse um Größenordnungen, wo dies sicher und rechtsstaatlich möglich ist.
- Bis 2030 werden alle relevanten Verfahren vollständig digitalisiert, standardisiert und medienbruchfrei organisiert.
- KI wird zur Vorstrukturierung, Plausibilisierung, Risiko-indikatorenerkennung, Dokumentenprüfung und Priorisierung eingesetzt. Die finale Entscheidung bleibt bei verantwortlichen Stellen.
- Für KRITIS-nahe Bereiche wird eine schnelle Vertrauens-würdigkeitsprüfung eingeführt, die Unternehmen und Betreibern kurzfristig handlungsfähige Ergebnisse liefert.

- Verfahren werden risikobasiert und rollenspezifisch ausgestaltet: nicht jede Tätigkeit benötigt dieselbe Prüftiefe, aber jede sicherheitsrelevante Tätigkeit benötigt ein angemessenes Vertrauensniveau.
- Effizienz, Qualität und Akzeptanz der Verfahren werden quartalsweise anhand von Bearbeitungszeiten, Fehlerquoten, Nachprüfungsbedarf und Nutzerfeedback gemessen.

6. Konsolidierung der staatlichen Sicherheitsarchitektur

Das gegenwärtige „Wimmelbild" der deutschen Sicherheitsbehörden – mit zahlreichen parallelen Zuständigkeiten, ungeklärten Verantwortlichkeiten und redundanten Strukturen – ist dringend reformbedürftig.

Wir empfehlen:

- „Beweispflicht" wird umgekehrt: Nicht das Argument für Zusammenführung, sondern das Argument für Aufgabenteilung muss künftig begründet werden.
- BSI wird zur wirklichen Zentralstelle des Bundes im Bereich Cybersicherheit gegenüber Ländern und anderen Behörden aufgewertet.
- Anzahl redundanter Strukturen wird bis 2030 um mindestens 40 % reduziert; gleichzeitig werden Informationsflüsse messbar beschleunigt (z. B. durch definierte maximale Übermittlungszeiten).
- Die vollständige Strukturprüfung erfolgt bis 2027, erste Konsolidierungsmaßnahmen werden bis 2028 umgesetzt. Die Strukturprüfung könnte durch eine Kommission, bestehend aus Vertretern einerseits der relevanten Ministerien unter Einbindung externer Experten aus Zivilgesellschaft und Wissenschaft erfolgen. Eine reine

Binnenbetrachtung nur durch die betroffenen Behörden erscheint nicht zielführend.

- Fortschritte werden jährlich anhand von Effizienzkennzahlen und halbjährlich durch Umsetzungsberichte überprüft.

7. Definition einer klaren strategischen Ausrichtung des BSI

Mit der Diskussion über aktive Cyberabwehr und eine etwaige Stärkung des BKA stellt sich zunehmend die Frage, wohin sich das BSI entwickeln soll und wie seine langfristige Aufstellung gesichert wird. Soll das BSI auf operative Tiefe setzen oder eine breite, themenübergreifende Abdeckung anstreben? Diese strategische Weichenstellung muss offen und verbindlich diskutiert werden. Als Beispiel sei der Bereich Verbraucherschutz genannt, dessen Zuordnung heute bereits umstritten ist.

Wir empfehlen:

- Strategische Positionierung des BSI zu operativer Tiefe und ressortübergreifender Abdeckung wird bis 2027 verbindlich festgelegt und durch konkrete Leistungs-kennzahlen operationalisiert.
- Bis 2030 wird das BSI als zentrale Steuerungsinstanz etabliert, gemessen u. a. am Anteil koordinierter Maßnahmen und mittels Zufriedenheitsscore von Bund und Ländern.
- Die Zielerreichung wird jährlich evaluiert und Stakeholder-Zufriedenheit halbjährlich erhoben.

8. Konsolidierung staatlicher Forschungsinstitutionen

Die Forschungslandschaft im Bereich Cybersicherheit umfasst heute eine Vielzahl von Institutionen – von der Cyberagentur über die Bundesagentur für Sprunginnovationen (SPRIND) und Exzellenzclustern, Fraunhofer-Instituten bis hin zu Projektträgern. Dies ist nicht per se ein Problem, aber der mögliche Synergiegewinn durch stärkere Bündelung wird zu wenig genutzt. Mindestanspruch ist eine bessere Koordinierung der Aktivitäten der Forschungseinrichtungen auf ministerieller Seite (oder ausgelagert z.B. an Cyberagentur oder SPRIND).

Wir empfehlen:

- Es wird geprüft, ob und wo größere Einheiten höhere Durchschlagskraft und stärkere Synergieeffekte entwickeln könnten. Ziel ist ein optimiertes Forschungsökosystem mit kürzeren Entwicklungszyklen, realen Testumgebungen und kontinuierlichen Fördermöglichkeiten.
- Synergieeffekte werden durch Kennzahlen wie verkürzte Entwicklungszyklen und erhöhte Anzahl gemeinsamer Projekte messbar gemacht.
- Erste strukturelle Bündelungen werden bis 2028 umgesetzt. Bis 2030 wird eine signifikante Effizienzsteigerung (z. B. Reduktion von Doppelstrukturen um ≥30 %) angestrebt.

- Wirkung wird jährlich anhand von Innovations- und Transferkennzahlen gemessen.

9. Strategie als dauerhafter Prozess: externe Partner verbindlich einbinden

Think Tanks wie die Stiftung Wissenschaft und Politik (SWP) werden bislang nur punktuell und projektbezogen in Strategieentwicklungen eingebunden. Das ist unzureichend. Strategie ist kein Projekt, sondern ein fortlaufender Prozess und muss so organisiert werden.

Wir empfehlen:

- Regelmäßiges und verbindliches Sparring mit zivilgesellschaftlichen Think Tanks, Wissenschaft und relevanten gesellschaftlichen Akteuren wird institutionell verankert. Das schafft Qualität durch zusätzliche Perspektiven und sichert Nachhaltigkeit.
- Einbindung externer Akteure wird durch klare Kennzahlen gesteuert (z. B. Anzahl strukturierter Austauschformate pro Jahr, Umsetzungsquote externer Empfehlungen).
- Bis 2027 werden verbindliche Formate etabliert und bis 2030 erfolgt eine institutionalisierte Einbindung mit messbarer Wirkung auf Strategiequalität.
- Zusammenarbeit wird jährlich evaluiert.

10. Schaffung eines Lagebilds der Cyberkompetenzen und -Ressourcen

Analog zu den Aktivitäten im Rahmen des Operationsplans Zivil (OPLAN Zivil) fehlt bislang eine systematische Erhebung der Cybersecurity-Ressourcen von Wirtschaft, Bund, Ländern und Kommunen.

Wir empfehlen:

- Zivil-militärische Zusammenarbeit (ZMZ) für den „Cyber-Verteidigungsfall" wird mit klaren Kompetenz-abgrenzungen zwischen Bundeswehr sowie ziviler Seite geplant und verankert.
- Planvollerer Austausch von Personal zwischen CIR, BSI und anderen Behörden – gegebenenfalls mit festen Rotations-zyklen.
- Idee eines „Cyberhilfswerks" zur Bürgerbeteiligung sollte in einem auf nationale Krisenlagen fokussierten Rahmen neu diskutiert werden.
- Bis 2027 wird eine vollständige Erfassung der nationalen Cyberressourcen erreicht. Bis 2028 erfolgt eine kontinuierliche Aktualisierung.
- Einsatzfähigkeit im Krisenfall wird durch einen „Response Capacity Index" messbar gemacht und jährlich bewertet.
- Datenbasis wird halbjährlich aktualisiert und jährlich umfassend analysiert.

11. Verbindliche Verankerung gemeinsamer Übungen und Sektoren-SPOCs

Analog zu Aktivitäten im Finanzsektor und bei UP KRITIS sollten alle Branchen regelmäßig an gemeinsamen Übungen mit staatlichen Institutionen teilnehmen. Diese Ansätze müssen auch innerhalb von UP KRITIS deutlich intensiviert werden, immer noch wird zu stark in Sektorengrenzen gedacht. Die Umsetzung hängt zu stark von intrinsischer Motivation einzelner Branchen ab. Als Positivbeispiel sei hier die Versicherungsbranche und deren Verband GDV genannt. Die Öffnung von UP KRITIS für alle NIS2-betroffenen Sektoren und Unternehmen ist ein wichtiger Schritt, der nun durch konkrete Aktivitäten fortgesetzt werden muss.

Wir empfehlen:

- Alle Branchen werden verpflichtet, sektorspezifische Single Points of Contact (SPOCs) einzurichten – nach dem Vorbild des GDV in der Versicherungswirtschaft – und an regelmäßigen Gemeinschaftsübungen teilzunehmen.
- Diese Übungen ergänzen bestehende Formate wie LÜKEX und bieten durch tiefere Sektordurchdringung und geringere Vorbereitungsaufwände einen eigenständigen Mehrwert.
- Bis 2027 werden SPOCs in allen KRITIS-Sektoren etabliert; ab 2028 finden jährlich verpflichtende sektorübergreifende Übungen statt.

- Reaktionsfähigkeit wird durch Kennzahlen wie Reaktionszeit und Umsetzungsquote von Verbesserungsmaßnahmen gemessen.
- Nach jeder Übung erfolgt eine strukturierte Auswertung; jährlich wird eine Gesamtbewertung erstellt.

12. Schaffung von IT-Sicherheitsmindest-standards für Parteien und Fraktionen

Parteien und ihre Fraktionen auf Bundes-, Landes- und kommunaler Ebene sind Teil der demokratischen Infrastruktur und de facto auch Kritische Infrastruktur. Ihre Absicherung muss dieser Tatsache Rechnung tragen.

Wir empfehlen:

- Verbindliche IT-Sicherheitsmindeststandards werden für Parteien und Fraktionen auf allen staatlichen Ebenen eingeführt und konsequent durchgesetzt.
- Einhaltung der Mindeststandards wird durch Auditquoten und Sicherheitsbewertungen messbar gemacht.
- Bis 2028 werden 100 % der relevanten Organisationen überprüft und normkonform gestellt. Die Überprüfung erfolgt jährlich.

13. Wirksamkeit und Verbindlichkeit der Bundesrechnungshof-Berichte sichern

Die substanziell hochwertigen Berichte des Bundesrechnungshofes zu Sicherheitsmängeln und IT-Defiziten bleiben bislang ohne unmittelbare Konsequenzen oder politischer Berücksichtigung. Das Potenzial dieser Erkenntnisse wird nicht ausgeschöpft.

Wir empfehlen:

- Behebung der vom Bundesrechnungshof festgestellten Missstände wird verbindlich, etwa durch den Einsatz von Maßgabebeschlüssen des Haushaltsausschusses des Deutschen Bundestages.
- Umsetzungsquote identifizierter Maßnahmen wird als zentrale Kennzahl definiert und soll bis 2028 mindestens 80 % betragen.
- Fortschritte werden halbjährlich überwacht und jährlich berichtet.

14. Einrichtung eines Cyber Safety Review Boards

Die systematische Auswertung von Sicherheitsvorfällen zur Prävention künftiger Angriffe fehlt in Deutschland bislang. Das muss sich ändern.

Wir empfehlen:

- Es wird ein Cyber Safety Review Board eingerichtet, das dem Nationalen Sicherheitsrat zugeordnet ist und Erkenntnisse aus Sicherheitsvorfällen institutionell verarbeitet und breit teilt. Dies muss in enger Einbindung des BSI-Lagezentrums geschehen.
- Das Board kann perspektivisch auch über klassische Cybersicherheitsvorfälle hinaus tätig werden und Sicherheitsaspekte in IT-Großprojekten und Software-lieferketten analysieren. Auch, um zu verhindern, dass Probleme wie bei der Einführung der elektronischen Patientenakte sich bei der EUDI-Wallet oder ähnlichen Vorhaben wiederholen.
- Anzahl analysierter Vorfälle sowie Zeit bis zur Veröffentlichung von Erkenntnissen werden als KPIs definiert.
- Bis 2028 wird eine umfassende Wissensbasis aufgebaut. Bis 2030 ist diese als Standardinstrument etabliert.

- Veröffentlichungen erfolgen quartalsweise. Wirkung wird jährlich bewertet.
- Die Implementation eines Abhängigkeitsmonitorings für kritische Softwarekomponenten wird eingeführt.
- Für den Fall kompromittierter Updates sind Notfallverfahren zu schaffen.
- Ergebnisse des Review Boards sollten – soweit sicherheitsrelevante Gründe nicht entgegenstehen – anonymisiert und in aggregierter Form veröffentlicht werden. Ziel ist es, sektorübergreifende Lernprozesse zu beschleunigen und die Resilienz des Gesamtsystems kontinuierlich zu erhöhen.

15. Vertrauensbildende Maßnahmen zwischen Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft

Die Bereitschaft zur Zusammenarbeit zwischen staatlichen Institutionen und gesellschaftlichen Akteuren im Bereich Cybersicherheit leidet erheblich unter mangelndem gegenseitigem Vertrauen. Verbändeanhörungen werden von der Wirtschaft häufig als Pflichtübung ohne echte Wirkung wahrgenommen.

Wir empfehlen:

- Staatliche Institutionen zeigen eine höhere Bereitschaft zu echter Zusammenarbeit mit Wirtschaft, Wissenschaft und Zivilgesellschaft auf Augenhöhe. Das schafft die Grundlage für mehr Engagement, bessere Meldebereitschaft und höheres Vertrauen in die Handlungsfähigkeit des Staates.
- Meldequote von Cybervorfällen sowie ein Vertrauensindex zwischen Staat und Wirtschaft werden als zentrale Kennzahlen etabliert.
- Bis 2030 wird eine signifikante Steigerung der Meldequote um mindestens 30 % gegenüber der 2026-Baseline angestrebt. Die 30 %-Zielgröße ist als politischer Mindest-ambitionswert festzulegen. NIS2 verpflichtet zu einem Frühwarnhinweis binnen 24 Stunden und zu einer vollständigen Meldung binnen 72 Stunden; ENISA betont, dass Incident Reporting zentral für Lagebild, Trendanalyse

und Resilienzsteigerung ist. Gemessen wird daher nicht nur die absolute Zahl der Meldungen, sondern die Melde-abdeckung je adressierter Organisation, Vollständigkeit, Fristtreue und Nutzbarkeit der Meldungen für Lagebild und Unterstützungsmaßnahmen.

Ergänzt wird dieser Vertrauensindex durch eine wissenschaftliche Erhebung des Dunkelfeldes auch bei nichtmeldepflichtigen Unternehmen.

- Eine jährliche Messung der Entwicklung.

16. Offensivere Kommunikation staatlicher Fähigkeiten

In Teilen der Wirtschaft und Gesellschaft besteht noch immer der Eindruck, staatliche Institutionen seien im Bereich Cybersicherheit nicht „wettbewerbsfähig", trotz unbestreitbarer Erfolge etwa bei der Bekämpfung von Cyberkriminalität. Das reduziert nicht nur die Meldebereitschaft, sondern untergräbt auch das Vertrauen in die Handlungsfähigkeit des Staates insgesamt.

Wir empfehlen:

- Eine offensivere und selbstbewusstere Außenkommunikation der eigenen Fähigkeiten und Erfolge – sowohl auf Ebene der einzelnen Sicherheitsbehörden als auch bis hin zum Nationalen Sicherheitsrat. Dies stärkt das subjektive Sicherheitsempfinden, erhöht die Meldebereitschaft und verbessert die Personalgewinnung.
- Wahrnehmung und Vertrauen in staatliche Cyberkompetenz werden durch regelmäßige Umfragen messbar gemacht.
- Bis 2030 wird eine deutliche Verbesserung der Wahrnehmungswerte angestrebt.
- Eine jährliche Messung der Entwicklung.

17. Konsequente Ausnutzung des Sanktionsrahmens

Die durch das BSI-Gesetz geschaffenen Sanktionsmöglichkeiten gegenüber Produktherstellern und IT-Dienstleistern werden bislang zu wenig genutzt. Es ist nicht zu erwarten, dass dies bei CRA und NIS2 anders sein wird.

Wir empfehlen:

- Unternehmen, die absichtlich oder grob fahrlässig die Sicherheit ihrer Kunden und der Gesellschaft gefährden, werden konsequent sanktioniert und dies transparent kommuniziert.
- Es geht nicht darum, Unternehmen mit leichter Fahrlässigkeit einem strengen Strafregime zu unterwerfen, sondern schwere und vorsätzliche Fälle klar zu ahnden.
- Anwendung und erste Messungen erfolgen ab 2028.

18. Integration eines Cybersecurity-Strangs in Wehrpflicht und Reserve

Technische Talente, die körperlich nicht für den klassischen Wehrdienst geeignet sind, werden unter dem heutigen Musterungsansatz nicht erfasst. Das verschenkt erhebliches Potenzial für die nationale Cyberverteidigungsfähigkeit.

Wir empfehlen:

- Eigenständiger Cybersecurity-Strang wird in die Wehrpflicht und die Reserve integriert. Als Vorbild kann die Cyberlegion in Polen dienen. Der Musterungsansatz wird entsprechend überarbeitet, sodass technische Eignung als eigene Kategorie Berücksichtigung findet.
- Anzahl rekrutierter Cyberfachkräfte sowie deren Einsatzfähigkeit werden als zentrale KPIs definiert.
- Bis 2030 wird ein signifikanter Aufbau entsprechender Kapazitäten angestrebt (z. B. mehrere tausend qualifizierte Kräfte).
- Fortschritte werden jährlich gemessen.

B) Schutz von Ländern und Kommunen

19. Klare Verantwortlichkeiten und Führungsstrukturen auf Landes- und Kommunalebene

Länder und Kommunen bilden die operative Frontlinie staatlicher Cybersicherheit. Sie betreiben einen Großteil der öffentlichen IT-Infrastruktur, erbringen zentrale Dienstleistungen für Bürgerinnen und Bürger und sind zunehmend Ziel professioneller Cyberangriffe. Die Resilienz Deutschlands im Cyberraum entscheidet sich daher nicht allein auf Bundesebene, sondern maßgeblich in den föderalen Strukturen vor Ort.

Viele Länder und Kommunen sind heute organisatorisch und strategisch untersteuert. Zuständigkeiten für Cybersicherheit sind fragmentiert, häufig nebenamtlich organisiert und ohne klare Durchgriffsbefugnisse.

Die zunehmende Digitalisierung staatlicher Leistungen erhöht die Abhängigkeit von funktionsfähigen IT-Systemen erheblich. Gleichzeitig fehlen in vielen Verwaltungen klare Führungsstrukturen, um Sicherheitsrisiken frühzeitig zu erkennen, Prioritäten zu setzen und im Krisenfall schnell handlungsfähig zu sein.

Wir empfehlen:

- Jedes Land etabliert eine klare politische und administrative Gesamtverantwortung für Cybersicherheit (z. B. CISO auf Staatssekretärsebene).
- Kommunen erhalten eindeutige Ansprechpartner-Strukturen mit klarer Eskalationslogik zum Land.
- Cybersicherheit wird als Daueraufgabe der Verwaltungsführung verankert, nicht als IT-Unterthema.
- Verbindliche Verantwortungsmodelle werden bundesweit vergleichbar gemacht.
- Bis 2028 haben 100 % der Länder eine politisch-administrative Gesamtverantwortung für Cybersicherheit benannt; bis 2030 verfügen 90 % der Kommunen über dokumentierte Eskalationswege zum Land.
- Jährliche Föderal-Governance-Erhebung; Indikatoren sind benannte CISO-/Koordinationsrollen, Vertretungsregelungen, Eskalationskontakte und getestete Erreichbarkeit.

20. Etablierung einer verbindlichen Bund-Länder-Kommunen-Governance für Cybersicherheit

Cybersicherheit im föderalen System leidet weniger an fehlenden Akteuren als an fehlender verbindlicher Orchestrierung zwischen Ebenen.

Die bestehenden Gremien und Kooperationsformate schaffen zwar Austausch, führen aber häufig nicht zu verbindlichen Entscheidungen oder einheitlichen Umsetzungsstandards. Dadurch entstehen Verzögerungen, Doppelstrukturen und Sicherheitsunterschiede zwischen den föderalen Ebenen.

Wir empfehlen:

- Etablierung einer ständigen föderalen Governance-Struktur für Cybersicherheit unterhalb des Nationalen Sicherheitsrates.
- Klare Rollenverteilung zwischen Bund (Strategie, Standards, Lagebild), Ländern (Betrieb, Unterstützung) und Kommunen (Umsetzung).
- Verbindliche Abstimmungs- und Eskalationsmechanismen statt freiwilliger Koordination.
- Cybersicherheit wird als föderale Gemeinschaftsaufgabe begriffen, nicht als delegierte Bundesaufgabe.

- Bis 2027 ist eine ständige Bund-Länder-Kommunen-Governance eingerichtet; ab 2028 werden mindestens vier strukturierte Lage-, Standard- und Eskalationsformate pro Jahr durchgeführt.

21. Etablierung verbindlicher Mindest-standards für Länder und Kommunen

Das Sicherheitsniveau öffentlicher IT-Systeme variiert stark zwischen Ländern und Kommunen. Freiwilligkeit führt zu strukturellen Schutzlücken.

Cyberangreifer orientieren sich regelmäßig am schwächsten Glied einer Sicherheitskette. Große Unterschiede beim Schutzniveau einzelner Verwaltungen gefährden deshalb nicht nur die betroffene Institution, sondern die Resilienz des gesamten staatlichen Systems.

Wir empfehlen:

- Einführung bundesweit verbindlicher Cybersicherheits-Baselines für Länder und Kommunen idealerweise auf Basis von NIS2 oder ähnlicher Regularien. Hierfür muss möglichst ein Weg gefunden werden, der dies ohne Grundgesetzänderung erlaubt.
- Orientierung an klar priorisierten Kontrollpunkten (Identitäten, Endpunkte, Daten, Steuerungsebenen).
- Mindeststandards sind technologieoffen, aber wirkungsspezifisch definiert.
- Verstärkte Rolle des BSI als Referenzgeber und Prüfinstanz gegenüber Ländern.

- Bis 2028 erfüllen 80 % der Länder und mindestens 60 % der Kommunen eine bundesweit definierte Cyber-Baseline; bis 2030 steigen die Quoten auf 100 % der Länder und 85 % der Kommunen.

22. Schaffung sicherer kommunaler Datenräume und von Interoperabilität

Kommunale Zusammenarbeit erfordert Datenaustausch, um eine effiziente und effektive Verwaltung zu ermöglichen. Unsicherer oder blockierter Datentransfer schwächt Verwaltungshandeln und Krisenfähigkeit und schwächt das Vertrauen der Bürger in die Fähigkeiten und Zuverlässigkeit der Verwaltung

Wir empfehlen:

- Aufbau sicherer, standardisierter Datenräume für föderale und kommunale Zusammenarbeit.
- Klare Regeln für Zugriff, Nutzung und Weitergabe von Daten implementieren.
- Sicherheitsarchitektur umsetzen, die Kooperation und gezielten Datenaustausch fördert und Abschottung nicht zum Regelfall macht.
- Interoperabilität wird als Sicherheitsfaktor begriffen, nicht als Risiko.
- Erfahrungen aus Projekten wie Gaia-X sollten genutzt werden, um darauf aufbauend belastbare Modelle zu entwickeln.
- Bis 2028 sind mindestens drei föderale Referenz-Datenräume produktiv erprobt; bis 2030 nutzen 70 % der Länder und 50 % der größeren Kommunen standardisierte Zugriff-, Protokollierungs- und Interoperabilitätsprofile.

23. Konsolidierung des IT-Betriebs der Kommunen

Die heutige IT-Betriebslandschaft auf kommunaler Ebene ist hochgradig fragmentiert und durch eine Vielzahl kleiner, isolierter Betriebsstrukturen geprägt. Viele Kommunen betreiben eigene, kleinteilige IT-Umgebungen, die weder über die notwendige Skalierung noch über ausreichende personelle und finanzielle Ressourcen verfügen, um ein angemessenes Sicherheitsniveau dauerhaft sicherzustellen. Eine langfristig resiliente und leistungsfähige kommunale IT kann daher nur durch eine konsequente Konsolidierung und Professionalisierung der Betriebsstrukturen erreicht werden. (siehe dazu auch die nachfolgende Forderung)

Wir empfehlen:

- Ab 2027 Konsolidierung des IT-Betriebs von Kommunen unterhalb eines definierten Größen- bzw. Leistungs-Schwellenwertes. Muster ist hierfür der Konsolidierungs-prozess, den die Sparkassen am Anfang der 2000er Jahre durchgeführt haben, in dem IT-Dienstleistungen bei der Finanz Informatik konzentriert wurde.
- Zulassung des Eigenbetriebs nur noch gewähren, wenn definierte Sicherheits- und Betriebsfähigkeitsstandards erfüllt werden. Kommunen, die diese Anforderungen nicht erfüllen können, müssen in konsolidierte Strukturen überführt werden.

24. Etablierung zentral verfügbarer Sicherheitsdienste für Kommunen

Parallel zu der grundsätzlichen Konsolidierung des kommunalen IT-Betriebs sollen zentrale Sicherheitsdienste etabliert werden. Kleine und mittlere Kommunen können moderne Sicherheitsfunktionen weder personell noch finanziell eigenständig betreiben. Dies dient einerseits als „Brückentechnologie“ für den parallel erforderlichen Konsolidierungsprozess, kann aber auch langfristig von den verbleibenden (großen) nicht konsolidierten Kommunen genutzt werden.

Wir empfehlen:

- Aufbau landesweiter oder länderübergreifender Security Shared Services (SOC, CERT, Identity Services).
- Kommunen erhalten niedrigschwelligen Zugang zu professionellen Sicherheitsleistungen.
- Skaleneffekte werden systematisch genutzt, Doppelstrukturen vermieden.
- Betrieb und Steuerung verbleiben in öffentlicher Hand oder unter klarer staatlicher Aufsicht.
- Bis 2028 haben 70 % der Kommunen Zugang zu landesweiten oder länderübergreifenden SOC-/CERT-/Identity-Shared-Services; bis 2030 nutzen mindestens 80 % der Kommunen mindestens einen solchen Dienst produktiv.

25. Finanzierung von Cybersicherheit als Pflichtaufgabe

Cybersicherheit auf kommunaler Ebene scheitert häufig nicht am Willen, sondern an struktureller Unterfinanzierung.

Mit der fortschreitenden Zentralisierung kommunaler und landesweiter IT-Landschaften steigt ihre Bedeutung als sicherheitskritische Infrastruktur. Ein erfolgreicher Angriff auf einen großen IT-Dienstleister kann heute unmittelbare Auswirkungen auf zahlreiche Behörden und öffentliche Leistungen haben.

Wir empfehlen:

- Anerkennung von Cybersicherheit als dauerhafte Pflichtaufgabe von Ländern und Kommunen.
- Zweckgebundene Finanzierungsinstrumente für Sicherheits-Baselines und Betrieb.
- Keine projektförmige Einmalförderung, sondern nachhaltige Betriebsfinanzierung.
- Transparenz über Mittelverwendung und Sicherheitswirkung.
- Bis 2028 wird Cybersicherheit in allen Ländern als dauerhaft zu finanzierende Aufgabe abgebildet; bis 2030 sind zweckgebundene Finanzierungsinstrumente für Baselines und Betrieb eingerichtet.

26. Strategische Neudefinition der Rolle der IT-Dienstleister der Länder

Landes- und kommunale IT-Dienstleister sind zentrale operative Akteure der staatlichen Cyberabwehr, werden aber häufig als reine Betriebsorganisationen verstanden.

Wir empfehlen:

- IT-Dienstleister der Länder werden explizit als kritische Sicherheitsakteure definiert.
- Sicherheitsverantwortung, Sicherheitsbefugnisse und Sicherheitsanforderungen werden klar geregelt.
- Enge Anbindung an Landes-CERTs, Sicherheitszentren und das BSI.
- Stärkere Bündelung und Arbeitsteilung zwischen IT-Dienstleistern verschiedener Länder.
- Die „NIS2-Betroffenheit“ der Dienstleister könnte als Basis angenommen werden und damit die Sicherheitsgrundlagen geschaffen werden.
- Bis 2028 sind 100 % der Landes-IT-Dienstleister als sicherheitsrelevante Akteure klassifiziert und an Landes-CERTs sowie das nationale Lagebild angebunden.

27. Schaffung einheitlicher Sicherheits-anforderungen an kommunale IT-Dienstleister

Das Sicherheitsniveau ausgelagerter IT-Services variiert stark, mit direkten Risiken für kommunale Handlungsfähigkeit.

Wir empfehlen:

- Einführung verbindlicher Sicherheitsanforderungen für alle IT-Dienstleister von Ländern und Kommunen.
- Orientierung an bundesweit einheitlichen Baselines und Referenzarchitekturen.
- Regelmäßige Überprüfung und Transparenz über das erreichte Sicherheitsniveau.
- Öffentliche IT-Dienstleister fungieren als Multiplikatoren für Sicherheitsstandards in der Fläche.
- Bis 2028 gelten einheitliche Sicherheitsanforderungen für 100 % neuer Verträge mit IT-Dienstleistern von Ländern und Kommunen; bis 2030 sind 80 % der Bestandsverträge angepasst.

28. Qualifizierung, Personalbindung und Entlastung der Verwaltung

Der Fachkräftemangel trifft Länder und Kommunen besonders stark. Einzelne Experten können ganze Verwaltungen nicht absichern. Der Wettbewerb um Cybersecurity-Fachkräfte wird sich durch KI, Digitalisierung und geopolitische Spannungen weiter verschärfen. Öffentliche Arbeitgeber müssen deshalb stärker auf attraktive Karrierewege, Weiterbildung und organisatorische Entlastung setzen, statt Sicherheitsverantwortung auf wenige Spezialisten zu konzentrieren.

Wir empfehlen:

- Systematischer Kompetenzaufbau durch standardisierte Schulungs- und Qualifizierungsprogramme.
- Entlastung lokaler IT durch zentrale Services und klare Arbeitsteilung.
- Attraktive Karriere- und Wechselmodelle zwischen Bund, Ländern und Kommunen.
- Fokus auf organisatorische Resilienz, nicht auf individuelle Heldenmodelle.
- Überlegungen für attraktivere Vergütungsmodelle starten und umsetzen.
- Führungskräftequalifizierung für Bürgermeister und Behördenleiter.

- Bis 2028 absolvieren 80 % der kommunalen IT-Verantwortlichen und 60 % der Verwaltungsleitungen ein standardisiertes Cyber-Grundlagenprogramm; bis 2030 ist jährliche Auffrischung verpflichtend.

29. Definition klarer Schnittstellen zu Polizei-, Verfassungs- und Katastrophenschutzstrukturen

Cybervorfälle sind regelmäßig auch Sicherheits-, Strafverfolgungs- oder Krisenlagen. Die Schnittstellen zwischen IT-Sicherheit und klassischen Sicherheitsbehörden sind jedoch unzureichend definiert.

Wir empfehlen:

- Einheitliche Schnittstellen zwischen IT-Sicherheitsstrukturen und Polizei, Verfassungsschutz, Katastrophen- und Bevölkerungsschutz auf Landesebene.
- Klar definierte Übergänge zwischen Cybervorfall, Cybernotfall und Krise
- Gemeinsame Lagebilder und abgestimmte Kommunikationslinien im Ernstfall.
- Regelmäßige ressortübergreifende Übungen auf Landes- und kommunaler Ebene.
- Bis 2028 verfügen alle Länder über dokumentierte Schnittstellen zwischen IT-Sicherheit, Polizei, Verfassungsschutz sowie Katastrophen- und Bevölkerungsschutz; ab 2028 wird mindestens jährlich geübt.

30. Festlegung klarer Melde-, Unterstützungs- und Eingriffs-mechanismen im Cybervorfall

Im Ernstfall fehlen oft klare Abläufe zwischen Kommunen, Ländern und Bund – Zeitverluste erhöhen Schäden.

Wir empfehlen:

- Einheitliche Eskalations- und Meldeprozesse für Cyber-vorfälle auf allen föderalen Ebenen.
- Klare Kriterien, wann Länder oder Bund unterstützend oder koordinierend eingreifen.
- Vermeidung föderaler Zuständigkeitsdebatten im Krisenfall durch vorab definierte Prozesse und Zuständigkeiten.
- Regelmäßige Übungen unter realistischen Bedingungen.
- Bis 2028 sind einheitliche Melde- und Eskalationsprozesse in allen Ländern und mindestens 80 % der Kommunen eingeführt; Fristtreue wird an 24-/72-Stunden-Logiken aus NIS2 gespiegelt.

31. Institutionalisierung eines föderalen Krisenmanagements für Cyberlagen

Cyberkrisen eskalieren schnell über Verwaltungsebenen hinweg. Ein abgestimmtes föderales Krisenmanagement ist bislang nicht ausreichend institutionalisiert.

Wir empfehlen:

- Integration von Cyberlagen in bestehende Krisen- und Katastrophenmanagement-strukturen der Länder.
- Klare Entscheidungs- und Kommunikationswege zwischen Kommunen, Ländern und Bund.
- Vorab definierte Rollen für Ministerien, Sicherheits-behörden und IT-Strukturen.
- Cyberkrisen werden als Teil gesamtstaatlicher Resilienz-planung behandelt.
- Bis 2028 sind Cyberlagen in 100 % der Landeskrisenstäbe und relevanten Katastrophenschutzpläne integriert; bis 2030 finden jährliche föderale Cyber-Krisenübungen statt.

32. Aufbau einer föderalen Lern- und Wissensplattform für kommunale Cybersicherheit

Erfahrungen aus Vorfällen, Audits und Übungen werden bislang kaum systematisch geteilt.

Während Unternehmen und Sicherheitsgemeinschaften häufig von gemeinsamen Erfahrungswerten profitieren, werden Erkenntnisse aus kommunalen Vorfällen bislang nur begrenzt systematisch ausgewertet. Dadurch werden Fehler wiederholt und erfolgreiche Lösungsansätze nicht ausreichend skaliert.

Wir empfehlen:

- Aufbau einer föderalen Wissensplattform für Länder und Kommunen, um übergreifend das Wissen zu bündeln und das große Bild verfügbar machen.
- Systematische Aufbereitung von Vorfällen, Best Practices und Lessons Learned.
- Niedrigschwelliger Zugang für Kommunen, ohne Prangerlogik.
- Enge Anbindung an das Cyber Safety Review Board auf Bundesebene.
- Bis 2028 ist eine föderale Wissensplattform produktiv; bis 2030 werden mindestens 80 % der relevanten Vorfälle, Übungen und Audits mit Lessons Learned eingestellt.

C) Cybersicherheit als Wirtschaftspolitik

33. Staat als strategischer Ankerkunde für deutsche und europäische Anbieter

In einem Markt, in dem Referenzprojekte, Zertifizierungen und Betriebsnachweise über internationalen Markterfolg entscheiden, ist die öffentliche Beschaffung kein Nebenthema, sondern industriepolitisches Kerninstrument. Der öffentliche Sektor muss als Erstmarkt, Referenzkunde und Skalierungshebel für vertrauenswürdige deutsche und europäische Anbieter wirken. In der Hoheit über von der Wirtschaft generierte Steuergelder hat er hier eine Vorbildfunktion einzunehmen und den Standortfaktor als entscheidendes Beschaffungskriterium entsprechend zu gewichten. Im Fall digitaler Plattform- und Cybersicherheitsmärkte ist zudem zu berücksichtigen, dass sich häufig nicht die technologisch besten, sondern die marktbeherrschenden Lösungen durchsetzen. Nicht umsonst ist "The winner takes it all" eines der beherrschenden Marktprinzipien der IT-Wirtschaft. Die daraus entstehenden, monopolistischen Strukturen werden bislang in der Beschaffungspolitik nur unzureichend berücksichtigt, was als strukturelles Beschaffungsdefizit gewertet werden kann. Staatliche Reaktionen sollten daher differenziert erfolgen: Partnerschaft, wo sinnvoll. Regulierung, wo erforderlich. Gezielte Abschottung und Investitionen, wo Risiken überwiegen.

Wir empfehlen:

- Die durch das Vergabebeschleunigungsgesetz und die neue Sicherheitsausnahme (u.a. §§ 97, 107, 128 Abs. 2 GWB) geschaffenen rechtlichen Instrumente werden konsequent genutzt, um Souveränitätskriterien verbindlich in Beschaffungsentscheidungen zu integrieren.
- Souveränitätskriterien umfassen dabei nicht nur formale Zertifizierung, sondern Standort, Eigentumskontrolle, Drittstaatenzugriff, Support, Datenzugriff, Exit-Fähigkeit, Betriebsort und Rechtsraum.
- Staat tritt nicht nur als Nachfrager, sondern als agiler Erstkunde auf: Innovative Lösungen werden bereits in fortgeschrittenen Entwicklungsphasen (TRL 7–8) pilotiert. Vergabeverfahren werden stärker auf funktionale Zielvorgaben – definierte Sicherheitsniveaus und nationale Fertigungstiefe – ausgerichtet.
- Bis 2028 sollen mindestens 40 % des einschlägigen Beschaffungsvolumens von Bundesverwaltung (inkl. Bundesagentur für Arbeit, Deutscher Rente, Bundeswehr, den Sicherheitsbehörden des BMI, sowie Steuer- und Zollverwaltung, aber auch von Ländern und Kommunen) auf EU-Anbieterbasis entfallen.
- Bis 2030 mindestens 50 %, mit verpflichtendem Souveränitäts-Check in allen KRITIS-nahen Beschaffungen.

34. Stärkung einer Förderpolitik, die den tatsächlichen Markteintritt unterstützt

Deutschland fördert zu stark frühe Technologieentstehung und zu wenig Kommerzialisierung. Dies gilt gleichsam für Produktimplementierung, Zertifizierung und Skalierung. Für Cybersecurity-Unternehmen sind genau diese Phasen kapitalintensiv, weil Vertriebszyklen lang, regulatorische Anforderungen hoch und Integrationsanforderungen in KRITIS/Verwaltung besonders anspruchsvoll sind. Ergänzend muss die Förderung stärker mit Auftragsforschung verknüpft werden, die es Unternehmen ermöglicht, ihre Technologien gezielt für staatliche Bedarfe weiterzuentwickeln.

Wir empfehlen:

- Förderung wird stärker auf marktnahe Skalierungsphasen (TRL 7–9) ausgerichtet und mit „first customer readiness", Zertifizierungsbudget, Referenzkundenprogrammen und kontrollierten Betriebsumgebungen verknüpft.
- Förderung wird stärker mit Auftragsforschung verbunden, die es Unternehmen ermöglicht, ihre Technologien gezielt für staatliche Bedarfe weiterzuentwickeln. Erweiterte Nachnutzungsmöglichkeiten öffentlich geförderter Technologien sind zu schaffen.
- Bis 2028 sollen mindestens 35 % der einschlägigen Cyber-Förderung in marktnahe Skalierungsphasen fließen.

- Bis 2030 mindestens 50 %, mit mindestens 60 % der geförderten Unternehmen mit einem ersten Referenzkunden binnen 24 Monaten.

35. Aufbau einer Nationalen Beschaffungsplattform für zertifizierte Anbieter und konsequentes PPI

Eine zentrale Plattform senkt Suchkosten, erhöht Transparenz und reduziert die strukturelle Benachteiligung kleinerer Anbieter im öffentlichen Markt. Auf EU-Ebene wird zwischen PCP (Pre-Commercial Procurement) und PPI (Public Procurement of Innovative Solutions) unterschieden. Für Cybersicherheit ist oft eine PCP-PPI-Kette sinnvoll: Vorwettbewerbliche Entwicklung, danach skalierende Beschaffung. Public Procurement of Innovative Solutions ist auf EU-Ebene als Instrument für marktnahe Innovation bereits etabliert. Für Cybersicherheit ist das besonders relevant, weil Einsatzreife oft im Piloten hängen bleibt. Dies könnte in den derzeit vom BMDS entwickelten „Marktplatz Deutschland“ integriert werden.

Wir empfehlen:

- Nationale Beschaffungsplattform für zertifizierte Cybersecurity-Anbieter wird aufgebaut. Sie senkt Suchkosten, erhöht Transparenz und ermöglicht die systematische Nutzung von Public Procurement of Innovative Solutions (PPI).
- Angesichts der föderalen Beschaffungsstruktur Deutschlands sind flankierende Maßnahmen zur

Entbürokratisierung und Modernisierung der Vergabeprozesse erforderlich.

- Bis 2028 sollen mindestens 1.000 qualifizierte Anbieterprofile gelistet sein.
- Bis 2030 sollen mindestens 25 % aller einschlägigen Cyber-Beschaffungen des Bundes über die Plattform erfolgen.

36. Neuausrichtung und Erweiterung einer Exportinitiative und Imagekampagne „Cybersecurity - Made in Germany"

Für deutsche Sicherheitsanbieter ist Exportfähigkeit essenziell, weil der Heimatmarkt allein zu klein ist, um globale Skaleneffekte zu erzeugen. Deutschland besitzt einen Vertrauensvorteil bei Security, Compliance, industrieller Qualität und KRITIS-Erfahrung. Dieser wird bislang zu wenig systematisch vermarktet.

Wir empfehlen:

- Die bestehende Exportinitiative „IT-Security Made in Germany" wird grundlegend neu ausgerichtet. Nach einer systematischen Wirkungsanalyse wird ein kohärenter Maßnahmenplan entwickelt, der neben Herstellern auch institutionelle Anwender einbezieht und konkrete Nutzungsszenarien international Märkten sichtbar macht.
- Zusammenarbeit mit Referenzkunden sowie die Unterstützung bei Standardisierungsaktivitäten werden gestärkt.
- Bis 2028 sollen staatlich unterstützten Auslandsmarkteintritte verdoppelt werden.
- Bis 2030 soll die Exportquote der deutschen Cyber-Industrie um mindestens 25 % gegenüber 2026 erhöht werden.
- Bis 2035 muss die deutsche Präsenz in europäischen und transatlantischen Vergaben messbar gesteigert werden.

37. Aufbau nationaler Champions in Cloud, KI, Security und Quantencomputing

Nicht jeder Bereich lässt sich realistisch vollständig autonom abdecken. Ziel muss der Aufbau von europäisch eingebetteten Champions in strategischen Segmenten sein: souveräne Sicherheitsarchitekturen, Managed Security Services, Identity, Zero-Trust-Komponenten, sichere Cloud- und Edge-Stacks, industrielle KI und ausgewählte Quantum-Security-Felder.

Wir empfehlen:

- In klar definierten strategischen Kernsegmenten werden gezielt deutsche und europäische Champions aufgebaut, um heimische Wertschöpfung zu stärken und Abhängigkeiten von Drittstaaten zu reduzieren.
- Ein unterstützender Hebel sind die stark steigenden Verteidigungsausgaben der kommenden Jahre. Analog zum Vorgehen der USA sollten mindestens zehn Prozent davon in KI und andere disruptive Technologien fließen.
- Bis 2030 sollen mindestens fünf deutsch-europäische Champions mit mehr als 100 Mio. Euro Jahresumsatz entstehen.
- Förderinstrumente alleine reichen nicht. Es werden harmonisierte Standards, interoperable Zertifizierungsverfahren sowie skalierbare und grenzüberschreitend nutzbare öffentliche Beschaffungsprozesse benötigt, um

einen funktionsfähigen europäischen Binnenmarkt für digitale Sicherheitslösungen zu schaffen. Ohne diesen Binnenmarkt ist langfristiger Erfolg europäischer Anbieter nicht möglich.

38. Erreichung einer Weltmarktführer-position in Post-Quantum-Kryptographie und spezialisierten KI-Systemen

Deutschland muss dort führen, wo sich Vertrauen, Sicherheit, Regulierungskompetenz und industrielle Tiefe in Wettbewerbsvorteile übersetzen lassen. Die bestehende Investitions- und Innovationslücke gegenüber den USA und China unterstreicht die Dringlichkeit dieser Stoßrichtung.

Wir empfehlen:

- Post-Quantum-Kryptographie (PQC) wird als nationales Prioritätsprojekt behandelt.
- Spezialisierte KI-Systeme für Sicherheitsanwendungen werden gezielt gefördert, insbesondere dort, wo industrielle Tiefe und regulatorische Kompetenz Wettbewerbsvorteile erzeugen.
- Strategischer Review zur internationalen Wettbewerbsposition gegenüber den USA und China findet alle zwei Jahre statt.
- Ab 2027 jährliches Monitoring von Quantum- und KI-Leitprojekten sowie technologischer Reifegrade (inkl. TRL-Bewertung und Markteintrittsstatus).
- Bis 2028 mindestens 5 industrielle Pilotanwendungen in Deutschland mit produktivem Einsatzbezug in Quantum- oder spezialisierten KI-Systemen.

- Erste systematische Erfassung des PQC-Transitionsgrads in kritischen Infrastrukturen.
- Bis 2030 mindestens 15–20 produktionsnahe Anwendungen in Industrie, KRITIS oder Verwaltung, mindestens 30 % der neu implementierten sicherheitskritischen Systeme mit Post-Quantum-Kryptographie-Komponenten, signifikante Steigerung der Patent- und Spin-off-Aktivität (Ziel: Verdopplung gegenüber 2027-Baseline).
- Alle 2 Jahre strategischer Review zur internationalen Wettbewerbsposition (insb. gegenüber USA/China) inklusive Anpassung der Förder- und Industriefokusfelder.
- Bis 2035 Etablierung von mindestens 1–2 global wettbewerbsfähigen europäischen Anbietern in ausgewählten Quantum-/AI-Sicherheitssegmenten, breite Marktdurchdringung von Post-Quantum-Kryptographie in europäischen KRITIS-Systemen (>60 %).

39. Stärkere Berücksichtigung von Industriepolitik beim Cyber Capacity Building

Capacity Building sollte nicht nur Entwicklungs-, Außen- oder Sicherheitspolitik sein, sondern auch markterschließende Industriepolitik. Wer Partnerstaaten bei CERT-Strukturen, SOC-Aufbau, Trainings, Identitäts- und Schutzarchitekturen unterstützt, prägt zugleich Standards, Lieferketten und Vertrauensräume. Das ist mit europäischen Zielen zu Sicherheit und Resilienz kompatibel, solange es offen, rechtskonform und interoperabel bleibt.

Wir empfehlen:

- Cyber Capacity Building wird stärker als kooperativer Ansatz zwischen staatlichen Institutionen und Unternehmen ausgestaltet. Unternehmen können im staatlichen Auftrag operative Leistungen erbringen und so gleichzeitig zur internationalen Markterschließung beitragen.
- Bis 2028 sollen mindestens 50 % der geförderten Programme mit deutscher oder europäischer Anbieterbeteiligung umgesetzt werden.
- Bis 2030 wird Capacity Building systematisch mit Exportförderung und Standardisierung verzahnt.

40. Etablierung praxisnaher Zertifizierungspfade und Schaffung eines Sicherheitslabels GER × EU

Für kleine und mittelständische Unternehmen (KMU) ist der Flaschenhals häufig nicht die technische Qualität, sondern der Nachweis von Vertrauenswürdigkeit. Der EU Cybersecurity Act (CRA) schafft einen unionsweiten Zertifizierungsrahmen, der für den Mittelstand durch praxisnahe und kosteneffiziente Wege ergänzt werden muss.

Wir empfehlen:

- Aufbauend auf dem European common criteria-based cybersecurity certification scheme (EUCC) werden praxisnahe, kosteneffiziente und marktwirksame Zertifizierungspfade für KMU entwickelt, die den Marktzugang zu KRITIS und Verwaltung erleichtern. Ergänzend werden Nachweise wie ISO/IEC 27001, BSI IT-Grundschutz oder CRA-Konformität einbezogen.
- Nationales „Fast-Track"-Programm für Zertifizierung wird gestartet. Bis 2028 sollen mindestens 500 KMU mit einem standardisierten Nachweis ausgestattet sein. Die Zertifizierungsdauer soll bis 2030 um 50 % gegenüber 2026 sinken.
- Die Anzahl und Qualität eingesetzter zertifizierter Sicherheitslösungen fließt in die Bewertung von

Unternehmen ein und wird als vergaberelevantes Kriterium berücksichtigt.

41. Übernahme von Führungsrollen in internationalen Standardisierungsgremien

Standardisierung ist Marktordnungspolitik. Wer technische Normen, Prüfverfahren und Interoperabilitätsprofile mit formt, prägt spätere Beschaffung, Compliance und Exportfähigkeit. Die EU-Standardisierungsstrategie von 2022 stellt genau diesen Zusammenhang zwischen Standards, Wettbewerbsfähigkeit und Resilienz heraus. Gleichzeitig ist zu berücksichtigen, dass die Struktur der deutschen IT-Sicherheitsanbieter nicht optimal auf die Mechaniken internationaler Standardisierungsgremien ausgerichtet ist. Große, global agierende Unternehmen verfügen hier über strukturelle Vorteile, systemische Wettbewerber wie China verfolgen eine industrieübergreifende Standardisierungsstrategie. Eine gezielte Unterstützung deutscher und europäischer Anbieter ist daher erforderlich und kann mit einer Neuausrichtung der Exportinitiative verknüpft werden.

Wir empfehlen:

- Deutsche und europäische Anbieter werden systematisch bei der Beteiligung an internationalen Standardisierungsgremien unterstützt (DIN/DKE, CEN/CENELEC, ETSI, ISO/IEC JTC 1/SC 27, IETF, NIST etc.).
- Unterstützung wird mit der Neuausrichtung der Exportinitiative verknüpft.

- Bis 2028 sollen die deutschen Führungsrollen in relevanten Gremien verdoppelt und eine entsprechende Baseline definiert werden.
- Bis 2030 ist eine sichtbare Co-Leadership in priorisierten Feldern anzustreben.

42. Verbesserung der Kapitalverfügbarkeit für Cybersecurity-Unternehmen

Der Kapitalzugang ist für Cybersecurity-, Cloud-, KI- und Deep-Tech-Unternehmen ein strategischer Engpass. Der deutsche und europäische VC-Markt zeigt strukturelle Defizite, insbesondere in späteren Finanzierungsphasen, was dazu beiträgt, dass erfolgreiche Unternehmen zu häufig ins Ausland abwandern.

Wir empfehlen:

- Steuerliche Rahmenbedingungen und Abschreibungsregeln für VC-Investitionen in Cybersicherheit und Deep Tech werden verbessert. Bis 2028 sollen Seed- und Series-A-Volumen verdoppelt werden; bis 2030 soll ein deutlicher Anstieg beim Wachstumskapital erreicht werden.
- Europäische Initiativen wie ein „Sovereign Tech Fund" sowie eine stärkere Rolle öffentlicher Investitionsbanken werden geprüft.

43. Aufbau eines PPP-Cyberfonds

Die Kommission KI & Wettbewerb des Bundeswirtschafts-ministeriums schlägt einen Staatsfonds "Deutsches Zukunftskapital" vor, welcher von 2026-2035 mit einem Volumen von ca. 300 Milliarden Euro ausgestattet werden soll. Der vorgeschlagene Fonds ist industriepolitisch plausibel, wenn er im Kern Sicherheitsrelevanz, Souveränität, Kommerzialisierung und Anschlussfinanzierung verankert ist und privates Kapital mobilisiert. Ein Teil des Zukunftsfonds sollte als Cyberfonds dediziert sein, mit Fokus auf Deep-Tech- und radikale Innovationsfelder, insbesondere auf KI-native Sicherheitslösungen und quantensichere Technologien. Der inhaltliche Fokus muss regelmäßig evaluiert und angepasst werden. Zusätzlich sollte geprüft werden, inwiefern Hochleistungsrecheninfrastruktur als „Computing Capital“ für Start-ups bereitgestellt werden kann, um kapitalintensive Entwicklungsphasen zu unterstützen.

Wir empfehlen:

- Dedizierter Cyberfonds wird als Teil des geplanten Zukunftsfonds aufgesetzt, mit klarem Fokus auf Deep-Tech- und radikale Innovationsfelder: KI-native Sicherheitslösungen, quantensichere Technologien und sicherheitsrelevante Infrastruktur.
- Fonds verankert im Kern die Dimensionen Sicherheits-relevanz, Souveränität, Kommerzialisierung sowie

Anschlussfinanzierung und mobilisiert aktiv privates Kapital.

- Zusätzlich wird geprüft, inwiefern Hochleistungs-Rechenzentrumsinfrastruktur als „Computing Capital" für Start-ups bereitgestellt werden kann.
- Bis 2030 sollen mindestens 50 Unternehmen gefördert sein, mit einer Folgefinanzierungsquote von über 60 %.

D) Digitale Souveränität

44. Schaffung eines verbindlichen Prüfschemas für kritische digitale Abhängigkeiten

Abhängigkeiten sind in digitalen Systemen normal – gefährlich werden sie dort, wo Transparenz, Exit-Fähigkeit, Redundanz oder Eingriffsmöglichkeit fehlen. Wer heute Verantwortung trägt, muss mehr wissen als nur, was eine Lösung technisch kann.

Wir empfehlen:

- Ein verbindliches Prüfschema für kritische digitale Abhängigkeiten wird eingeführt, das überall dort verpflichtend angewendet wird, wo Technologien Zugriff auf strategische Kontrollpunkte haben: Endpunkte, Identitätsinfrastrukturen, Datenräume, Kollaborations- und Cloud-Steuerungsebenen sowie sicherheitskritische Betriebsservices. Wo dies EU-Recht berührt, bemüht sich Deutschland um eine entsprechende europaweite Regelung.
- Das Prüfschema umfasst fünf Herkunftsfragen, die als fester Bestandteil eines erweiterten Risikochecks zu verstehen sind:
    - Wo wird die Technologie entwickelt?
    - Wo wird sie betrieben?

    - Wo wird der Service erbracht?
    - Woher kommen Geschäftsführung und Aufsicht?
    - Wer sind die Investoren?
- Diese Fragen ersetzen keine Sicherheitsarchitektur, ergänzen aber technisches Risikomanagement dort, wo Jurisdiktion und Verantwortungsstruktur operative Handlungsfähigkeit beeinflussen.
- Bis 2028 wird das Prüfschema in 100 % kritischer Beschaffungen und Architekturentscheidungen angewandt; bis 2030 liegen für alle strategischen Kontrollpunkte aktuelle Abhängigkeitsprofile vor.

45. Definition und Umsetzung verbindlicher Resilienz-Baselines

Kritische Funktionen müssen auch bei Angriffen, Ausfällen oder Störungen arbeitsfähig bleiben. Dazu fehlen heute meist verbindliche Mindeststandards, die schnelle Schutzwirkung entfalten.

Wir empfehlen:

- Für Staat, Kritische Infrastrukturen und Mittelstand wird ein Mindestniveau definiert und umgesetzt, das auf schnelle Schutzwirkung zielt: Identitäten härten, Endpunkte sichern, Segmentierung, Logging, Backup und Recovery, Vorfallkommunikation und regelmäßige Übungen.
- Diese Baselines setzen direkt an den strategischen Kontrollpunkten an. Ziel ist nicht die Vermeidung jeder Störung, sondern die Fähigkeit, Wirkung zu begrenzen und Handlungsfähigkeit zu garantieren.
- Verbindliche Referenzarchitekturen und Mindeststandards für datenzentrierte Sicherheit werden etabliert, um Interoperabilität und sichere Zusammenarbeit über Organisationsgrenzen hinweg zu ermöglichen.
- Bis 2028 erfüllen 80 % der Bundesbehörden, 70 % der KRITIS-nahen Organisationen und 50 % des adressierten Mittelstands die definierte Mindestbaseline; bis 2030 jeweils 95 %, 85 % und 70 %.

46. Konsequente Priorisierung strategischer Kontrollpunkte

Die Debatte über Cybersicherheit ist oft zu breit. Das verlangsamt Entscheidungen und verwässert Wirkung. Operativ verdichtet sich digitale Souveränität an wenigen Stellen, an denen sich tatsächliche Steuerungsfähigkeit entscheidet.

Wir empfehlen:

- Investitionen, Regulierung und Architekturentscheidungen werden priorisiert entlang der vier strategischen Kontrollpunkte ausgerichtet: Endpunkte, Identitäten, Datenräume und zentrale Steuerungsebenen. Wer Identitäten kontrolliert, kontrolliert Zugriff. Wer Endpunkte kontrolliert, kontrolliert Ausführung. Wer Datenräume kontrolliert, kontrolliert Wertschöpfung.
- Dieses Prinzip der Priorisierung gilt ausdrücklich auch für die föderale Umsetzung: Was überall gleich sein muss – Sicherheits-Baselines, Prüfschemata für Abhängigkeiten, Mindestanforderungen an Datenkontrolle – ist verbindlich zu standardisieren. Was variabel bleiben kann (konkrete Technologien, Betriebsmodelle, organisatorische Umsetzung) bleibt dezentral. Die Priorisierung dieser Kontrollpunkte dient zugleich der gezielten Konzentration von politischen, finanziellen und organisatorischen Ressourcen. Dadurch wird sichergestellt, dass Investitionen

dort erfolgen, wo sie die größte systemische Hebelwirkung entfalten.

- Ab 2027 werden mindestens 70 % neuer Cyber-Investitionen explizit einem der vier Kontrollpunkte zugeordnet; bis 2030 erreichen alle kritischen Programme einen Kontrollpunkt-Wirkungsnachweis.

47. Verankerung des Leitprinzips datenzentrierter Sicherheitsarchitektur

In verteilten, cloudbasierten und KI-gestützten Systemen lässt sich Kontrolle nicht mehr allein über Netzgrenzen und Systemperimeter herstellen. Sicherheit muss sich von einer primär infrastrukturbasierten Logik hin zu einer datenzentrierten Logik entwickeln.

Wir empfehlen:

- Sicherheitsarchitekturen werden darauf ausgelegt, kontrolliertes Teilen zu ermöglichen, statt zu verhindern: kontrollierte Datenräume statt isolierter Silos, nachvollziehbare Nutzung statt pauschaler Abschottung, standardisierte Zugriffskonzepte statt individueller Sonderlösungen.

  Ein Beispiel ist der Austausch von Lage- und Bedrohungsinformationen zwischen Staat, KRITIS-Betreibern und Unternehmen im Cybervorfall: Heute bleiben relevante Informationen häufig noch in organisatorischen Silos oder können nur verzögert geteilt werden; moderne datenzentrierte Sicherheits-architekturen ermöglichen, dass solche Informationen kontrolliert, rollenbasiert und nachvollziehbar ausgetauscht und gemeinsam genutzt werden können

- Entscheidend ist die Fähigkeit, Datenflüsse und deren Nutzung regelbasiert zu steuern – auch über Organisationsgrenzen hinweg. Es muss klare Regeln geben, wer Daten sehen, verändern, weitergeben darf oder für welche Zwecke sie verwendet werden. Diese Regeln müssen technisch durchsetzbar und nachvollziehbar sein.
- Data-Centric Security wird damit zur Voraussetzung für funktionierende Datenräume und neue kollaborative Geschäftsmodelle zwischen Staat, Wirtschaft und Gesellschaft.
- Bis 2028 sind für priorisierte Datenräume verbindliche Policy-as-Code-, Rollen-, Protokollierungs- und Zweckbindungsprofile definiert; bis 2030 werden 70 % kritischer Datenaustausche danach gesteuert.

48. Aufbau eines europäisch integrierten Zero-Trust-Stacks zur Erreichung technologischer Souveränität

Deutschland und Europa sind in zentralen Bereichen der digitalen Sicherheitsinfrastruktur von proprietären Systemen und nicht-europäischen Anbietern abhängig. Das ist ein strategisches Risiko, aber kein Argument für Protektionismus, sondern für strategische Klarheit.

Wir empfehlen:

- Ein klar definierter Analyserahmen wird entwickelt, der sachlogisch bestimmt, in welchen Teilbereichen technologische Souveränität notwendig ist und in welchen nicht.
- Nationale und europäische Sicherheitslösungen werden entlang einer gemeinsamen Zero-Trust-Architektur integriert. Offene Standards und interoperable Schnittstellen ermöglichen die sichere Zusammenarbeit von Identitäts-, Daten- und Sicherheitsdiensten über Organisations- und Landesgrenzen hinweg und reduzieren die Abhängigkeit von proprietären Plattformen.
- Das Ziel ist ein nationales und europäisches Sicherheitsökosystem, das auf vertrauenswürdige Endgeräte, souveräne Cloud-Infrastrukturen und kontrollierbare Betriebsmodelle setzt – und dabei

Offenheit und Kontrolle nicht als Gegensatz, sondern als zwei Seiten derselben Architektur versteht.

- Anteil klassifizierter Datenbestände, technisch durchgesetzte Zugriffsregeln, Auditierbarkeit, Zahl kontrollierter organisationsübergreifender Datennutzungen und Verstöße gegen Nutzungsregeln.
- Bis 2028 liegt ein europäisch anschlussfähiger Zero-Trust-Referenzstack für kritische Einsatzbereiche vor; bis 2030 verfügen 60 % kritischer Neuarchitekturen über dokumentierte substituierbare Komponenten und Exit-Pfade.

49. Aufbau einer Nationalen Cyber-Architekturplattform mit Service-Katalog und Marketplace

Viele Unternehmen, Kommunen und öffentliche Einrichtungen wissen grundsätzlich, dass sie ihre Cybersicherheit verbessern müssen. Was ihnen häufig fehlt, ist ein einfacher, vertrauenswürdiger und handlungsorientierter Weg von der Standortbestimmung zur Umsetzung. Der Markt ist unübersichtlich, Standards sind komplex, Beratungsangebote heterogen und konkrete technische Maßnahmen schwer vergleichbar. Gerade Mittelstand, Kommunen und kleinere KRITIS-nahe Organisationen benötigen daher keine weitere abstrakte Strategie, sondern einen kuratierten Zugang zu überprüfbaren Architekturen, geprüften Services und konkreten Umsetzungspfaden.

Wir empfehlen den Aufbau einer nationalen Cyber-Architekturplattform nach dem Vorbild eines „Well-Architected Framework“ für Cybersicherheit. Organisationen sollten dort ihre Cyberstance entlang weniger zentraler Dimensionen selbst oder begleitet überprüfen können: Identitäten, Endpunkte, Datenflüsse, Backup und Recovery, Logging, Segmentierung, Lieferketten, Cloud-Steuerungsebenen und Krisenfähigkeit. Ziel ist kein weiteres Audit-Regime, sondern ein pragmatisches Instrument zur schnellen Selbsteinschätzung, Priorisierung und Verbesserung.

Die Plattform sollte drei Funktionen verbinden.

Erstens einen standardisierten Cyberstance-Check. Organisationen erhalten anhand eines einfachen Reifegradmodells eine Einschätzung ihrer Sicherheitslage, ihrer größten Risiken und der nächsten wirksamsten Schritte. Dieser Check sollte an bestehenden Standards wie BSI IT-Grundschutz, ISO/IEC 27001, NIS2, CRA und branchenspezifischen Anforderungen anschlussfähig sein, aber deutlich einfacher und handlungsorientierter gestaltet werden.

Zweitens einen kuratierten Architektur- und Service-Katalog. Für typische Organisationstypen – Kommune, Schule, Krankenhaus, Mittelstand, KRITIS-Betreiber, Verband, Partei, Forschungseinrichtung – werden Referenzarchitekturen und Mindestpakete bereitgestellt. Diese sollten konkrete Schutzwirkungen beschreiben: sichere Identität, gehärteter Endpunkt, kontrollierter Datenraum, sicheres Backup, Notfallkommunikation, Monitoring und Incident Response.

Drittens einen vertrauenswürdigen Marketplace für geprüfte Anbieter und Services. Unternehmen und öffentliche Einrichtungen sollten auf Basis ihres Cyberstance-Checks unmittelbar passende, vorqualifizierte Services beziehen können: Endpoint-Härtung, Identity Management, Managed Detection and Response, Backup/Recovery, Awareness-Schulungen, sichere Kollaboration, Schwachstellenscans, Notfallübungen oder Beratungsleistungen. Der Marketplace sollte nicht nur Anbieter listen, sondern nach

Schutzwirkung, Zertifizierungsstatus, Souveränitätskriterien, Betriebsmodell und Zielgruppe kuratieren.

Ein solcher Ansatz hätte drei Vorteile. Er würde erstens die Umsetzung von Cybersicherheit drastisch vereinfachen, weil Organisationen nicht bei null anfangen müssten. Er würde zweitens öffentliche und private Nachfrage bündeln und dadurch den Cybermarkt strukturieren. Und er würde drittens digitale Souveränität operationalisieren, indem Sicherheitsarchitekturen, Souveränitätskriterien und konkrete Services miteinander verbunden werden.

Wir empfehlen:

- Aufbau einer nationalen Cyber-Architekturplattform als gemeinsames Instrument von BSI, Wirtschaft, Ländern und relevanten Branchenverbänden.
- Entwicklung eines einfachen, anschlussfähigen Cyberstance-Checks entlang strategischer Kontrollpunkte: Identitäten, Endpunkte, Datenräume und Steuerungsebenen.
- Bereitstellung kuratierter Referenzarchitekturen und Baseline-Pakete für Kommunen, Mittelstand, KRITIS, Parteien, Schulen und öffentliche Einrichtungen.
- Aufbau eines geprüften Service-Katalogs und Marketplace für vertrauenswürdige Cybersecurity-Services.
- Verknüpfung mit bestehenden Zertifizierungs-, Förder- und Beschaffungsinstrumenten, damit Organisationen aus der Diagnose unmittelbar in Umsetzung kommen.

- Nutzung von KI zur automatisierten Ersteinschätzung, Maßnahmenpriorisierung, Dokumentation und kontinuierlichen Verbesserung der Cyberstance.
- Bis 2028 sind mindestens 5.000 Organisationen im Cyberstance-Check registriert und 1.000 geprüfte Services im Katalog; bis 2030 erfolgen 25 % einschlägiger öffentlicher Cyber-Beschaffungen über die Plattform.

E) Bildung von der Kita bis zur Seniorenresidenz

Die zuvor geforderte souveräne Cybernation braucht souveräne Cyberbürger. Und zwar auf allen Ebenen. Eine Bevölkerung, die souverän mit der Technologie und den damit verbundenen Risiken und Chancen umzugehen weiß. Und aus der heraus sich ausreichend Fachkräfte entwickeln lassen. Dies bedingt parallel dazu, dass wir es uns als Land nicht erlauben können, Potential dadurch zu verlieren, weil der Anteil an weiblichen Fachkräften so gering bleibt, wie er aktuell ist. Es geht also hier nicht nur um Schulbildung, sondern auch um Awareness und die gezielte Ansprache von Frauen und Mädchen, um diese für alle Themen rund um MINT zu begeistern.

Bei aller Notwendigkeit technischer Maßnahmen:

Der Cyberdome beginnt nicht im Netz, sondern in den Köpfen.

50. Massive Investitionen in MINT-Ausbildung und Lehrkräftequalifizierung

Deutschland ist es über die Jahrhunderte immer gelungen, die Veränderungen und Neuanforderungen in der Wirtschaft bzgl. der erforderlichen Kompetenzen der Arbeitskräfte im Schulsystem abzubilden. Dies war immer ein wesentlicher Erfolgsfaktor unserer Wirtschaft und auch Teil des Aufstiegsversprechens an die Bevölkerung.
Sei es im 18. Jahrhundert bei der 1. Industriellen Revolution, wo durch die aufkommenden Maschinen Arbeiter statt Bauern benötigt wurden und dem gestiegenen Bildungsbedarf durch die Schul-/Unterrichtspflicht entsprochen wurde.

Sei es im 19. Jahrhundert bei der 2. Industriellen Revolution, wo durch die fortschreitende Industrialisierung und das Aufkommen von Fabriken mit einhergehender Aufgabenteilung eine stärkere Diversifizierung und Spreizung der Bildungsanforderungen erforderlich wurde und Deutschland das dreigliedrige Bildungssystem einführte.

Sei es im 20. Jahrhundert, wo in der 3. Industriellen Revolution durch Automatisierung und Einzug von Elektronik Berufe immer höhere Spezialkenntnisse erforderlich machten und Deutschland mit dem dualen Bildungssystem die passende Antwort bereithielt.

Vor dem Hintergrund dieser Erfolgsgeschichte ist es umso unverständlicher und dramatischer, dass im 21. Jahrhundert es immer noch nicht gelungen ist, auf die 4. Industrielle Revolution, die flächendeckende Digitalisierung, eine vergleichbare Antwort zu finden. Wo gleichzeitig über Fachkräftemangel, nachlassende Innovativität und schwindende Wettbewerbsfähigkeit unserer Volkswirtschaft geklagt wird, ist es geradezu ein Staatsversagen, die so offensichtliche Basis dieses Problems über Jahrzehnte zu ignorieren.

Das Argument, dass Änderungen nur auf Kosten anderer Lehrinhalte möglich wären, die aber gleichfalls Berechtigung haben und eine solche Verdrängung nicht erwünscht ist, halten wir für nicht zielführend. Jedes Fach hat seine Berechtigung, es muss aber erlaubt sein, über die Verteilung zu sprechen. Diese Diskussionen wurden auch schon vor über 100 Jahren geführt und wenn man damals nicht den Mut zu Änderungen gehabt hätte, würden wir heute vermutlich noch den Homer in Altgriechisch auswendig können, aber nicht die drittgrößte Volkswirtschaft sein.

Wir empfehlen:

- Massive Investitionen in MINT-Ausbildung und Lehrkräfte-qualifizierung, u.a. durch Programme zur Frühförderung von MINT-Talenten in Grund- und Mittelstufe ab 2027
- Aufbau respektive Ausweitung eines bundesweiten Weiterbildungsprogramms für Lehrkräfte ab 2027

51. Einführung von Informatik als durchgängiges Pflichtfach in allen Bundesländern

Bis heute ist Informatik nicht in allen Bundesländern Pflichtfach. Und dort, wo es obligatorisch ist, ist es nicht über die gesamte Schullaufbahn präsent. Die stiefmütterliche Behandlung des Themas Informatik als Schulfach über Jahrzehnte führt dazu, dass auch dort, wo das Fach angeboten wird, durch den simplen Mangel an angemessen ausgebildeten Lehrkräften nicht in der benötigten Qualität durchgeführt werden kann. Das sprichwörtliche Erstellen eine Powerpoint-Präsentation ist nicht der benötigte Lehrinhalt, um die diagnostizierten Defizite zu beheben. Leider ist es eher die Regel als die Ausnahme, dass Mathematik- oder Physik-Lehrkräfte als Informatik-Lehrkräfte eingesetzt werden müssen. Ein Französisch-Lehrer ist kein Spanisch-Lehrer, auch wenn es verwandte Sprachen sind. Gleiches gilt auch für MINT-Fächer. Wenn zu diesem Fachkräfteproblem dann auch noch schnell veraltende Lehrpläne und stiefmütterlich behandelte Themenbereiche dazukommen, ist die Qualität des Unterrichts und des Lernerfolgs leicht zu prognostizieren.

Um im Bild zu bleiben: Sprachen ändern sich und entwickeln sich weiter. Aber nicht so schnell wie das Thema Informatik. Hier muss der Takt der Lehrplan-Aktualisierung massiv erhöht werden. Dies ist für einzelne Bundesländer nicht möglich. Und auch nicht sinnvoll. Wer Bildungsföderalismus als Vorteil durch

Diversifizierung und Wettbewerb der Bundesländer versteht, versündigt sich im Zeitalter einer sich exponentiell beschleunigenden Digitalisierung und eines massiv steigenden Wettbewerbsdrucks durch die Globalisierung an unseren Kindern und unserer Wirtschaft.

Wir empfehlen:

- Schaffung eines bundesweiten Pflichtfachs Informatik bis zum Jahre 2028.
- Fortschritte werden halbjährlich anhand von Abdeckungs-, Lehrkräfte- und Unterrichtsquoten evaluiert.
- Bis 2030 wird Informatik als durchgängiges Unterrichtsfach von der 1. bis zur 12. Klasse etabliert; der Umsetzungsgrad wird jährlich gemessen.
- Bis 2028 wird Informatik in 100 % der Bundesländer als verpflichtendes Schulfach eingeführt.
- Erweiterung des Pflichtfachs zu einem durchgängigen Unterrichtsfach von der 1. bis zur 12. Klasse bis 2030.

52. Verbindliche Verankerung von Cybersicherheit im Informatik-Lehrplan

Das Thema Cybersicherheit ist nicht in allen Lehrplänen in den Bundesländern vertreten, und selbst wo dies der Fall ist, ist der Inhalt oft nicht angemessen, veraltet und bekommt einen zu geringen Anteil.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt, bis zu 20 % des IT-Budgets für Cybersicherheit einzuplanen. Dies soll nicht als Kennzahl für den Anteil am Gesamt-Curriculum übernommen werden, deutet aber an, dass der aktuelle im niedrigen einstelligen Prozentsatz zu niedrig ist.

Wir empfehlen:

- Schaffung einer deutschlandweiten Taskforce bis 2028, die die bestehenden Informatik-Lehrpläne vereinheitlicht und aktualisiert und hierin das Thema Cybersicherheit angemessen und modern abbildet. Dies ist kein Projekt, sondern ein dauerhafter Prozess, um dem steigenden Änderungstempo in der Digitalisierung eine adäquate Antwort geben zu können. An der föderalen Bildungshoheit kann und darf dieses Thema nicht scheitern.
- Anteil qualifizierter Informatik- und Cybersecurity-Lehrkräfte soll bis 2030 signifikant gesteigert werden und wird jährlich gemessen.

- Aktualisierung der Lehrpläne erfolgt mindestens jährlich. Die Synchronisierung mit Hochschulen und Weiterbildungsprogrammen wird halbjährlich überprüft.
- Bis 2028 wird eine bundesweite Taskforce etabliert und ein harmonisierter Cybersecurity-Lehrplan für alle Länder verabschiedet.
- Diese stetigen Änderungen müssen jederzeit mit den Hochschulen bzgl. der Lehrerausbildung und zusätzlichen Weiterbildungsprogrammen für die aktiven Lehrer synchronisiert werden.

53. Aufbau eines Quereinsteigerprogramms für Informatiklehrer

Alle Lehrpläne auf dem Papier sind nur so gut wie die Menschen, die die Inhalte vermitteln. Und hier haben wir einen dramatischen Mangel an Fachkräften. Dies wird auch nur langfristig zu beheben sein. Gleichzeitig sehen wir, dass durch den Siegeszug der künstlichen Intelligenz gerade Stellen für Anwendungsentwickler gefährdet sind. Hier entfallen bereits heute – mit massiv steigender Geschwindigkeit – Stellen. Was negativ klingt, ist aber auch eine Chance. Technisch ausgebildete Menschen müssen sich am Arbeitsmarkt neu orientieren. Dies kann und sollte in zwei Richtungen stattfinden. Wir können die bestehenden Kompetenzen so erweitern, dass neue Fachkräfte für die Cybersicherheit bereitstehen, wir können diese Menschen aber auch versuchen, für Lehrberufe zu gewinnen.

Wir empfehlen:

- Wirksamkeit des Programms wird anhand von Besetzungsquoten und Unterrichtsausfall jährlich evaluiert.
- Anzahl erfolgreich qualifizierter und dauerhaft eingesetzter Lehrkräfte wird als zentrale KPI definiert und jährlich berichtet.

- Bis 2028 wird ein bundesweites Quereinsteigerprogramm etabliert; Ziel ist die Qualifizierung mehrerer tausend zusätzlicher Informatiklehrkräfte bis 2030.
- Schaffung und aktive Bewerbung eines Umschulungs-/Weiterbildungsprogrammes bis 2028, das hilft, IT-Fachkräfte wie etwa Anwendungsentwicklern für den Einsatz als Lehrkräfte zu qualifizieren.

54. Einrichtung eines Ausbildungsberufs „Fachinformatiker(in) Cybersicherheit“

Einer der großen Erfolgsfaktoren der deutschen Wirtschaft ist die Ausbildung der Fachkräfte auch jenseits der akademischen Bildungswege. Weltweit werden wir um unser duales Ausbildungssystem beneidet Von daher ist es komplett unverständlich, dass genau bei der Cybersicherheit dies nie genutzt wurde, sondern ausschließlich auf die akademische Bildung gesetzt wurde. Dieses fatale Fehlen eines kompetenten “Mittelbaus” spürt gerade auch der deutsche Mittelstand, der kaum Fachpersonal für die erforderlichen konzeptionellen und administrativen Aufgaben findet. Das bisher stets verwendete Argument, dass in den bestehenden Fachinformatiker-Ausbildungsgängen das Thema Cybersicherheit abgedeckt wird, entspricht nicht den Anforderungen bzgl. notwendiger Spezialisierung in der Praxis.

Wir empfehlen:

- Schaffung eines expliziten Ausbildungsweges für Cybersicherheit. Derzeit läuft hier in NRW ein erstes Pilotprojekt auf Initiative von eurobits und der CISO Alliance. Dies ist bis 2028 bundesweit auszurollen.
- Bis 2030 soll eine signifikante Steigerung verfügbarer Cybersecurity-Fachkräfte im Mittelstand erreicht werden.

- Anzahl neu geschaffener Ausbildungsplätze sowie erfolgreich abgeschlossener Weiterbildungsprogramme wird jährlich gemessen.
- Bis 2028 wird der Ausbildungsberuf „Cybersicherheit“ bundesweit eingeführt und in allen relevanten Ausbildungsstrukturen verankert.
- Aus den entstehenden Lehrplänen sind Kurzlehrgänge abzuleiten, die es z.B. Fachinformatikern für Systementwicklung, deren Berufsaussichten sich aktuell wie oben beschrieben durch die KI massiv verschlechtern, ermöglichen sich schnell und berufsbegleitend für einen entsprechenden neuen Abschluss weiterzubilden.
- Cybersicherheit ist aber nicht ausschließlich ein technisches Berufsfeld. Ebenso entscheidend sind Kompetenzen in den Bereichen Management, Verwaltung, Recht und Regulierung. Insbesondere die Fähigkeit, technische Risiken organisatorisch, juristisch und strategisch einzuordnen, wird zu einem zentralen Engpassfaktor. Diese Kompetenzen müssen in andere Berufsbilder integriert werden.

55. Steigerung des Anteils weiblicher Fachkräfte

ISC² gilt als eine der wichtigsten Quellen für globale Cybersicherheits-Arbeitsmarktdaten. Bereits im Women-in-Cybersecurity Report 2024 schätzte sie den Frauenanteil in der Branche weltweit auf 20-25%. In Deutschland beträgt der Anteil weiblicher Cybersecurity-Fachkräfte gerade einmal knapp 15% .Im internationalen Vergleich liegt Deutschland damit am unteren Ende der G7-Staaten: Italien, 27%, Kanada 21%, USA 19%, UK 18%, Deutschland 15% (Frankreich und Japan nicht ausgewiesen).

Dieser Wert hat sich im Laufe der Zeit langsam verbessert – von lediglich 11 % im Jahr 2013 auf 24 % im Jahr 2022. Prognosen gehen davon aus, dass der Anteil bis 2031 weltweit auf etwa 35 % ansteigen könnte.

Diese Prognose stimmt zwar grundsätzlich optimistisch, ist aber kein Selbstläufer. Wir müssen hier aktiv werden, um den Rückstand zu anderen Ländern aufzuholen und deutliche Steigerungen zu erreichen.

Das es auch anders geht, zeigt uns leider die kriminelle Seite der Cybersicherheit: Untersuchungen von Trend Micro und Branchenberichte zeigen, dass der Frauenanteil in der kriminellen Untergrundszene bei etwa 30 bis 40 Prozent liegt. Damit ist die

Cybercrime-Szene deutlich diverser als die reguläre IT-Sicherheitsbranche.

Dies ist ein Zustand, der nicht akzeptabel ist. Und solange wir diesen nicht beheben, werden die ambitionierten Ziele dieser Strategie vermutlich nicht erreichbar sein.

Der Handlungsauftrag geht auch direkt an die Privatwirtschaft und ist keine reine Aufgabe an die Politik. Während in Deutschland bereits 19 % der Cybersicherheitsberater weiblich sind, sind es unter den CISOs nur 8 %. Man kann nicht über fehlende Fachkräfte klagen, wenn man sich offensichtlich teilweise bei der Suche ein Auge zuhält.

Wir haben dies schon bei der initiierenden Konferenz bildlich verdeutlicht:
„Wer sich 2040 vor staatlich gelenkten Cyberangriffen aus Russland, China & Co. schützen will, muss die heute achtjährigen Mädchen für MINT und Cybersecurity begeistern."

Aber es geht auch nicht nur um MINT-Kompetenzen. Die Cybersicherheit ist inhaltlich so breit gefächert, dass auch komplett andere Bildungswege - exemplarisch seien Politikwissenschaften, Psychologie und Journalismus genannt -in Karrieren in der Cybersicherheit münden können, z.B. im Krisenmanagement, Strategieentwicklung, Awarenessbildung, Risikoanalysen etc.

Dies ist aber den entsprechenden Absolventinnen (und natürlich auch Absolventen) nicht bekannt.

Wir empfehlen:

- Intensivierung mädchenspezifischer MINT-Förderung ab der Grundschule.
- Bis 2027 Einsetzung einer Kampagne an Hochschulen um Absolventinnen (und Absolventen) anderer Studiengänge auf die Möglichkeiten in der Cybersicherheit aufmerksam zu machen und aufzuzeigen, dass hier nicht nur Mathematik-Interessierte gesucht werden. Als Ideen seien hier genannt:
    - „Wer das Risiko von Vulkanausbrüchen bewerten kann, kann auch das Risiko von Hackereinbrüchen bewerten."
    - „Cyberangriffe machen etwas mit den Betroffenen. Wer macht etwas mit den Betroffenen?"
    - „Den größten Schaden bei Cybervorfällen richtet oft falsche Kommunikation an. Wer kann besser kommunizieren?"

- Bis 2028 Aufbau einer Kampagne mit weiblichen „Role Models"
- Ziel muss es sein, bis 2030 den Rückstand auf den globalen Durchschnitt aufzuholen, was prognostisch wie oben beschrieben einen Anteil von mindestens 30-35 % bedeutet.

- Zur Erreichung der Gesamtziele dieser Strategie sollte ein Anteil von 40 % als Mindestziel gelten, wobei das grundsätzliche Langfristziel natürlich 50 % sein sollten.

56. Ermöglichung und Förderung von ehrenamtlichem Engagement aus Wirtschaft und Gesellschaft

Selbst bei maximalem Einsatz ist klar, dass der Mangel an ausreichend ausgebildetem Fachpersonal nur langfristig zu schließen ist. Es reicht also nicht, hier nach dem Staat zu rufen und auf schnelle Lösungen zu hoffen. Wirtschaft und Gesellschaft sind hier parallel gefordert, und sei es nur, um eine "Brückenlösung" für die erforderliche Übergangszeit zu finden. Wir spüren in unseren Unternehmen bei den Mitarbeitern, aber auch außerhalb durch zivilgesellschaftliche Initiativen auch eine große Bereitschaft hierzu. Diese Bereitschaft muss nur gezielt zur Traktion gebracht werden.

Schon heute engagieren sich viele Eltern an den Schulen ihrer Kinder und Fachkräfte ohne Kinder im entsprechenden Alter wollen ebenfalls helfen.

Aktuell ist dies aber "Stückwerk" und beinhaltet die Gefahr, dass in erster Linie ohnehin schon privilegierte Kinder und Schulen profitieren, da die engagierten Eltern ob ihres Bildungsgrades ihre Kinder eben meist nicht an "Brennpunktschulen" haben. Vielen Schulen fehlt also schlicht der Zugang zu hilfsbereiten Fachkräften. Mitgliedsunternehmen des Wirtschaftsrates gehen hier bereits in Vorleistung: wir entwickeln eine Plattform, wo Schulen niedrigschwellig eine ehrenamtliche Fachkraft für Onlineunterricht

vermittelt bekommen. Als Projekttag oder als simple Option, um Stundenausfall durch langfristige Lehrerausfälle etc. zu begegnen.

Wir starten einen Pilotbetrieb, wo Schülerinnen und Schülern der 9.Klasse acht Stunden Cybersecurity-Unterricht angeboten werden sollen. Die Unterrichtseinheiten werden mit Videos und Material vorbereitet, um einheitliche Qualität zu gewährleisten. In Zusammenarbeit mit der Allianz für Cybersicherheit des BSI und führenden Wirtschaftsverbänden sollen die über 8.000 Mitgliedsunternehmen motiviert werden, ihre Mitarbeitenden für 8 Stunden pro Jahr kostenlos zur Verfügung zu stellen.

Wir empfehlen:

- Staatliche Unterstützung dieses Pilotprojektes ab 2026.
- Bei Erfolg Ausdehnung auf andere Jahrgänge und andere Themen.
- Wirkung und Reichweite werden jährlich anhand von Teilnahme-, Zufriedenheits- und Kompetenzindikatoren bewertet.
- Bis 2028 soll ein bundesweites Netzwerk mit messbarer Beteiligung von Unternehmen und Schulen aufgebaut werden.
- Pilotprojekt wird ab 2026 systematisch evaluiert. Anzahl teilnehmender Schulen, Unterrichtsstunden und ehrenamtlicher Fachkräfte werden als KPIs definiert.

57. Erstellung einer flächendeckenden, zielgruppenspezifischen und koordinierten Awareness-Kampagne

Bildungsbedarf besteht aber nicht nur für Schüler, sondern quer durch die gesamte Bevölkerung. Vereinfacht gesagt reduziert sich Schadenshöhe und auch Fachkräftebedarf auch dadurch, dass wir als Bevölkerung eine Art "Herdenimmunität" entwickeln. Hier existieren seit Jahren viele gute und lobenswerte Aktivitäten. Man muss aber auch konzedieren, dass viele dieser Aktivitäten eher aktionistisches Stückwerk ohne große Nachhaltigkeit sind. Ursache hierfür sind projekthafte Förderungen einzelner Projekte von einer Vielzahl von Fördermittelgebern und Einzelinitiativen. Es ist nie gelungen, einen koordinierten gesamtgesellschaftlichen Ansatz wie in den 60er/70er Jahren im Bereich Verkehrssicherheit ("Der 7. Sinn") oder in den 80er Jahren im Bereich AIDS-Aufklärung zu verfolgen und diesen auch angemessen finanziell zu unterfüttern. Die jährlich steigenden Zahlen im Bereich Cybercrime zeigen die Konsequenzen dieses Versäumnisses. Dies betrifft den Schaden von Privatpersonen, aber auch den von Unternehmen, denn es sind ja dieselben Menschen, die auf verschiedenen Ebenen angegriffen werden und sich davon überfordert zeigen.

Gleichzeitig zeigt sich oft die Hilfslosigkeit, wenn Sicherheitsexperten als Marketing-Laien an Zielgruppen vorbei informieren.

Wir empfehlen:

- In Anlehnung an die o.g. großen Aufklärungskampagnen zur Verkehrssicherheit („Der 7.Sinn“) und zur AIDS-Prävention wird ab 2027 eine konzertierte Aufklärungskampagne entwickelt, die Zielgruppen und Themen identifiziert und einen professionellen Kommunikationsplan mit Themen und Kanälen vom Fernsehspot für die Boomer bis zum Influencer für die Generation Z & Alpha mit klaren Reichweiten- und Wirkungskriterien umsetzt.
- BSI und DsiN könnten hier fachlich federführend und koordinierend wirken, es muss aber deutlich “größer gedacht” und professioneller als die bisherigen Ansätze werden. Ja, dies wird Millionen kosten. Aber es senkt Schäden um Milliarden. Wie schon oben postuliert, beginnt der Cyberdome nicht am Netzzugang, sondern in den Köpfen. Wenn 1 % des Budgets für den Cyberdome jährlich in dieses Thema fließen würde, prognostizieren wir einen höheren Wirkungsgrad als bei jedem anderen Teilbudget.
- Bis 2030 soll eine signifikante Verbesserung des gesellschaftlichen Cybersecurity-Bewusstseins sowie eine messbare Reduktion erfolgreicher Betrugs- und Cybercrime-Fälle erreicht werden.
- Reichweite, Wiedererkennungswert und Veränderung des Sicherheitsverhaltens werden jährlich durch repräsentative Studien gemessen.

- Ziel ist es, dass 2035 80 Prozent der Bevölkerung über ein Basiswissen Cybersicherheit verfügen, das über digitale Grundkenntnisse hinausgeht (in Anlehnung an die „Digital Decade Initiative der EU)

F) Prinzipien für einen nachhaltigen Erfolg

Bereits die Umsetzung einzelner der hier getätigten Empfehlungen als Einzelmaßnahmen wirkt positiv, die Umsetzung eines Großteils der Empfehlungen wäre ein großer Schritt nach vorne hin zur Cybernation. Sie allein sichern aber nicht, dass es danach nicht wieder zu einem Stillstand oder gar Rückschritten kommt.

Es bedarf eines grundsätzlichen Mindset-Wechsels.

Die Cybernation Deutschland kann nicht allein durch Einzelmaßnahmen, Institutionen oder Kennzahlen entstehen. In einer technologischen Umgebung, die sich durch KI, Automatisierung und geopolitische Veränderungen immer schneller wandelt, müssen Entscheidungen auch dort getroffen werden können, wo konkrete Regeln noch nicht existieren.

58. Entwicklung eines Cybernation-Prinzipienkatalogs

Um das erforderliche Mindset zu manifestieren, braucht es gemeinsame Prinzipien als dauerhaften Orientierungsrahmen für Staat, Wirtschaft und Gesellschaft. Aus diesem Grund empfehlen wir die Entwicklung eines Cybernation-Prinzipienkatalogs als gemeinsamem Orientierungsrahmen.

Der Anspruch der nachfolgenden Vorschläge ist es, diese Prinzipien in konkrete politische, institutionelle und wirtschaftliche Maßnahmen zu übersetzen und so die Grundlage für eine resiliente, souveräne und wettbewerbsfähige Cybernation Deutschland zu schaffen. Diese Prinzipien ersetzen keine Strategie und keine konkreten Maßnahmen. Sie schaffen jedoch eine gemeinsame Entscheidungslogik für Zielkonflikte: Sicherheit versus Geschwindigkeit, Souveränität versus globale Zusammenarbeit, zentrale Steuerung versus dezentrale Innovation. Erfolgreiche digitale Organisationen zeigen, dass wenige klare Prinzipien vielen Akteuren ermöglichen, auch unter Unsicherheit konsistent und schnell zu handeln.

Wir empfehlen:

- Entwicklung eines Cybernation-Prinzipienkatalogs bis 2027 durch einen strukturierten Prozess mit Staat, Wirtschaft,

Wissenschaft und Zivilgesellschaft, unter dem Dach des Bundeskanzleramtes.

- Durchführung von Szenario- und Krisensimulationen zur Validierung der Prinzipien, insbesondere für KI-Disruptionen, Cyberangriffe, Lieferkettenabhängigkeiten und hybride Bedrohungen.
- Erste Leitprinzipien sollten sein: Resilienz vor reiner Autarkie; Kontrolle strategischer Fähigkeiten statt Kontrolle aller Technologien; Sicherheit als Voraussetzung für Zusammenarbeit; bewusste Steuerung kritischer Abhängigkeiten; gemeinsame Verantwortung von Staat, Herstellern, Betreibern und Nutzern.
- Verankerung der Prinzipien in Digitalstrategien, Beschaffungsentscheidungen, Architekturvorgaben und Ausbildungsprogrammen der öffentlichen Verwaltung.
- Einrichtung eines jährlichen Cybernation Reviews, um Prinzipien anhand technologischer Entwicklungen und realer Krisenerfahrungen weiterzuentwickeln.

Schlussbetrachtung

Die Vorschläge dieses Papiers verstehen „Cybernation“ als eine holistische Aufgabe, die sich nicht in einzelne Politikfelder aufteilen lässt. Sicherheitsarchitektur, Souveränität und Wirtschaftspolitik sind keine voneinander getrennten Handlungsstränge – sie greifen ineinander und bedingen sich gegenseitig. Wer die staatliche Sicherheitsarchitektur modernisiert, ohne gleichzeitig einen leistungsfähigen Cybermarkt zu entwickeln, schafft Strukturen ohne Substanz. Wer digitale Souveränität fordert, ohne strategische Kontrollpunkte zu priorisieren und verbindliche Baselines durchzusetzen, betreibt Symbolpolitik. Und wer Wirtschaft fördert, ohne den Staat als glaubwürdigen Ankerkunden zu positionieren, finanziert Innovation ohne Wirkung.

Deutschland hat die intellektuellen, wirtschaftlichen und institutionellen Voraussetzungen, um in Europa eine tragende Rolle beim Aufbau einer souveränen digitalen Sicherheitsarchitektur zu spielen. Die Fähigkeit, an den entscheidenden Kontrollpunkten Kontrolle zu behalten, kritische Abhängigkeiten aktiv zu steuern und Sicherheit so zu bauen, dass Zusammenarbeit und staatliche Handlungsfähigkeit zugleich möglich bleiben, ist keine technische Frage – sie ist eine Frage politischen Willens und institutioneller Konsequenz.

Die Vorschläge dieses Papiers benennen, wo dieser Wille in konkrete Entscheidungen übersetzt werden muss. Es ist nun an der Politik, diesen Schritt zu tun.

Literaturverzeichnis

A. Primärquellen

A.1 Strategien und Politikdokumente

- Bitkom (2024): Wirtschaftsschutz 2024: Schäden durch Cyberangriffe in Deutschland. Berlin: Bitkom e.V. Verfügbar unter: https://www.bitkom.org (Zugriff: 24.04.2026).
- Bundesministerium für Bildung und Forschung (BMBF) (2018): Hightech-Strategie 2025: Forschung und Innovation für die Menschen. Berlin: BMBF. Verfügbar unter: https://www.bmbf.de (Zugriff: 24.04.2026).
- Bundesregierung (2023): Zukunftsstrategie Forschung und Innovation. Berlin: Bundesregierung. Verfügbar unter: https://www.bundesregierung.de (Zugriff: 24.04.2026).
- Bundesregierung (2025): Hightech Agenda Deutschland. Berlin: Bundesregierung. Verfügbar unter: https://www.bundesregierung.de (Zugriff: 24.04.2026).
- European Commission (2019): Regulation (EU) 2019/881 (Cybersecurity Act). Brüssel: Europäische Kommission. Verfügbar unter: https://eur-lex.europa.eu (Zugriff: 24.04.2026).
- European Commission (2022): An EU Strategy on Standardisation: Setting global standards in support of a resilient, green and digital EU economy. Brüssel: Europäische Kommission. Verfügbar unter: https://commission.europa.eu (Zugriff: 24.04.2026).

- European Commission (2023): The Digital Decade Policy Programme 2030. Brüssel: Europäische Kommission. Verfügbar unter: https://digital-strategy.ec.europa.eu (Zugriff: 24.04.2026).
- European Commission (2024): The Future of European Competitiveness (Draghi Report). Brüssel: Europäische Kommission. Verfügbar unter: https://commission.europa.eu (Zugriff: 24.04.2026).
- European Investment Bank (EIB) (2023): Innovation Finance Advisory: Supporting Innovation in Europe. Luxemburg: EIB. Verfügbar unter: https://www.eib.org (Zugriff: 24.04.2026).
- European Union Agency for Cybersecurity (ENISA) (2022): NIS Investments Report. Athen: ENISA. Verfügbar unter: https://www.enisa.europa.eu (Zugriff: 24.04.2026).
- European Union Agency for Cybersecurity (ENISA) (2023): Cybersecurity Maturity Assessment Framework. Athen: ENISA. Verfügbar unter: https://www.enisa.europa.eu (Zugriff: 24.04.2026).
- European Union Agency for Cybersecurity (ENISA) (2024): EU Cybersecurity Certification Framework (EUCC). Athen: ENISA. Verfügbar unter: https://www.enisa.europa.eu (Zugriff: 24.04.2026).
- EuroHPC Joint Undertaking (2024): European High Performance Computing Infrastructure. Luxemburg: EuroHPC JU. Verfügbar unter: https://eurohpc-ju.europa.eu (Zugriff: 24.04.2026).

- EuroStack Initiative (2025): EuroStack: A European Sovereign Technology Stack. Brüssel: EuroStack Initiative. Verfügbar unter: https://euro-stack.eu (Zugriff: 24.04.2026).
- KfW Research (2024): Venture Capital Markt Deutschland 2024. Frankfurt am Main: KfW. Verfügbar unter: https://www.kfw.de (Zugriff: 24.04.2026).
- Letta, E. (2024): Much More Than a Market. Brüssel: Europäischer Rat. Verfügbar unter: https://www.consilium.europa.eu (Zugriff: 24.04.2026).
- McKinsey & Company (2024): Quantum Technology Monitor. New York: McKinsey. Verfügbar unter: https://www.mckinsey.com (Zugriff: 24.04.2026).
- OECD (2021): Public Procurement for Innovation: Good Practices and Strategies. Paris: OECD Publishing. Verfügbar unter: https://www.oecd.org (Zugriff: 24.04.2026).

A.2 Regulatorische und technische Rahmenwerke

- European Union Agency for Cybersecurity (ENISA): EU Cybersecurity Certification Framework (EUCC)
  Online verfügbar: https://www.enisa.europa.eu
- European Commission: NIS2 Directive & Cyber Resilience Act (CRA)
  Online verfügbar: https://eur-lex.europa.eu

A.3 Markt-, Technologie- und Finanzierungsdaten

- Bitkom (2024): Wirtschaftsschutz 2024 – Schäden durch Cyberangriffe in Deutschland.
  Online verfügbar: https://www.bitkom.org
- KfW Research (2024): Venture Capital Markt Deutschland 2024.
  Online verfügbar: https://www.kfw.de
- McKinsey & Company (2024): Quantum Technology Monitor.
  Online verfügbar: https://www.mckinsey.com
- OECD (2021–2024): Public Procurement for Innovation.
  Online verfügbar: https://www.oecd.org
- TrendMicro:
  https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/gender-in-cybercrime
  (Zugriff: 08.06.2026).
- IT-Daily**:** https://www.it-daily.net/it-sicherheit/cloud-security/steigender-bedarf-an-cybersicherheitsexperten-frauen-stark-unterrepraesentiert

B. Sekundärliteratur

B.1 Analyse- und Referenzberichte

- Mario Draghi (2024): The Future of European Competitiveness (Draghi Report).
  Online verfügbar: https://commission.europa.eu
- Mario Draghi (2025): Speech on European Competitiveness and Technology.
  (zitiert bzgl. KI-Modelle und Investitionslücke)
- EuroStack Initiative (2025): EuroStack – A European Sovereign Technology Stack.
  Online verfügbar: https://euro-stack.eu
- Enrico Letta (2024): Much More Than a Market (Letta Report).
  Online verfügbar: https://www.consilium.europa.eu

B.2 Diskussions- und Kontextquellen

- European Investment Bank (EIB): Innovation Financing in Europe.
  Online verfügbar: https://www.eib.org
- EuroHPC Joint Undertaking: European High Performance Computing Infrastructure.
  Online verfügbar: https://eurohpc-ju.europa.eu

Wirtschaftsrat der CDU e.V.
Bundesgeschäftsstelle
Luisenstraße 44, 10117 Berlin
Telefon 030/24087-0
Telefax 030/24087-405
www.wirtschaftsrat.de
info@wirtschaftsrat.de

Impressum:
Wolfgang Steiger, Generalsekretär
Johannes Gunst, Geschäftsführer
Anne Schaaf, Geschäftsführerin
Diana Scholl, Geschäftsführerin
Simon Steinbrück, Geschäftsführer
Richard Yates, Geschäftsführer

Herausgeber:
Prof. Timo Kob,
Vorsitzender BFK Cybersicherheit
HiSolutions AG

Chefredaktion:
Katharina M. Schwarz, MYRA Security GmbH
Maik Hofmann, Wirtschaftsrat der CDU e.V.

Autorinnen und Autoren:
Katharina M. Schwarz, MYRA Security GmbH
Prof. Timo Kob, HiSolutions AG
Olaf Janssen, Sopra Steria SE
Peter Wirnsperger, Deloitte GmbH
Andreas Barke, HiSolutions AG
Michael Barth, genua GmbH
Ferdinand Gehringer, FTI Consulting
Dr. Sven Herpig, Interface
Andreas Könen, BIGS
Philipp Müller, DriveLock SE
André Roosen, Deloitte GmbH
Sofie Schönborn, Schwarz Digits KG