Der Beauftragte der
Bundesregierung
für Informationstechnik

Netzstrategie 2030 für die öffentliche Verwaltung

Bedarfsgerechte, leistungsfähige und sichere Netzinfrastrukturen für die öffentliche Verwaltung

Version 1.01 11/2018

Impressum

Herausgeber

Der Beauftragte der Bundesregierung für Informationstechnik

Ansprechpartner

Bundesministerium des Innern, für Bau und Heimat

Referat BMI CI 5 – Netzinfrastrukturen; Digitalfunk BOS

Postanschrift: Alt-Moabit 140, 10557 Berlin

Hausanschrift: Bundesallee 216-218, 10719 Berlin

CI5@bmi.bund.de

www.cio.bund.de

Stand

November 2018

Bildnachweis

Quelle Titelbild: www.alamy.de

Kurzfassung

Die Netzstrategie 2030 für die öffentliche Verwaltung (fortan: Netzstrategie) stellt die Fortschreibung der Gesamtstrategie IT-Netze der öffentlichen Verwaltung[1] aus dem Jahr 2013 dar und trägt den seitdem veränderten Rahmenbedingungen Rechnung. Zu diesen zählen das Projekt IT-Konsolidierung Bund, die Konsolidierung der Weitverkehrsnetze der Bundesverwaltung (Projekt Netze des Bundes (NdB)), die Konsolidierungen des IT-Betriebs und der Netze der jeweiligen Landesverwaltungen sowie die veränderte Cybersicherheitslage und erweiterte gesetzliche Rahmenbedingungen, wie bspw. das Onlinezugangsgesetz. Im Ergebnis ist die Landschaft der Weitverkehrsnetze der öffentlichen Verwaltung insgesamt heterogen, wodurch die Absicherung sowie digitale Zusammenarbeit erschwert werden. Die Netzstrategie konkretisiert das im Jahr 2013 für den Bund gesetzte Leitbild zum Eigenbetrieb sicherheitskritischer IT-Systeme und IT-Infrastrukturen durch ein Zielbild 2030 und skizziert den Informationsverbund der öffentlichen Verwaltung (IVÖV) als bedarfsgerechten, leistungsfähigen und sicheren Träger der föderalen Digitalisierung. Die getroffenen Festlegungen beziehen sich in diesem Rahmen auf die Weitverkehrsnetze der öffentlichen Verwaltung. Den strategischen Rahmen (Anforderungen, Ziele, strategische Handlungsfelder) für die Gestaltung des Zielbildes bilden die dieser Strategie vorangestellten Eckpunkte einer Netzstrategie 2030 für die öffentliche Verwaltung[2]. Sie wurden auf Ebene des Bundes im Rahmen der Konferenz der IT-Beauftragen (KoITB) abgestimmt, Vertretern von Ländern und Kommunen vorgestellt sowie abschließend dem IT-Planungsrat zum Beschluss empfohlen[3]. Das entwickelte Zielbild 2030 legt die Gestaltung des IVÖV in vier Dimensionen fest, die nachfolgend dargestellt werden.

Definition IVÖV
Aus Sicht der Einrichtungen der öffentlichen Verwaltung ist der IVÖV ein Netzverbund zwischen Nutzern (i. S. v. Einrichtungen) und Anbietern von IT-Diensten (i. S. v. Anwendungen und Fachverfahren) und dient der Kommunikation der gesamten öffentlichen Verwaltung von Bund, Ländern und Kommunen. Leistungen im Bereich Netzdienstleistungen (bspw. krisensichere Anschlüsse) und Sicherheit (bspw. Beratung, Überwachung der Sicherheit) werden durch die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) bzw. das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereitgestellt und, unter Wahrung der Unabhängigkeit im Föderalismus, in Form eines optionalen Angebots, der gesamten öffentlichen Verwaltung zur Verfügung gestellt. Das Angebot umfasst auch die Möglichkeit, die BDBOS mit dem Betrieb eines Landesnetzes zu beauftragen (Opt-In Entscheidung). Somit übernehmen die BDBOS und das BSI den Betrieb des Basisnetzes inklusive den jeweiligen Netzübergängen sowie für Netze von Ländern mit Opt-In Entscheidung.

Technische Architektur
Aus technischer Betreibersicht zählen grundsätzlich alle Weitverkehrsnetze der öffentlichen Verwaltung zu den verbundenen Netzen[4] im IVÖV. Im Einzelnen sind dies die verbundenen Netze der Bundesverwaltung und Netze der Auslands-IT des Auswärtigen Amtes, das Verbindungsnetz gem. IT-NetzG[5], die verbundenen Netze von Landes- und Kommunalverwaltungen sowie ggf. weitere

[1] Vgl. Bericht zur Gesamtstrategie der Netze der öffentlichen Verwaltung (2013).

[2] Der Beauftragte der Bundesregierung für Informationstechnik (2018): Eckpunkte einer Netzstrategie 2030 für die öffentliche Verwaltung.

[3] IT-Planungsrat (2018), Entscheidung 2018/52; Der IT-Planungsrat hat die Eckpunkte einer Netzstrategie 2030 in der 27. Sitzung am 25.10.2018 zur Kenntnis genommen. Die Zusammenarbeit von Bund, Ländern und Kommunen bei der weiteren Detaillierung der Strategie ist fortzuführen.

[4] Begriffsbestimmung siehe Glossar Anhang B: Verbundene Netze.

[5] Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder (i. V. m. Art. 91c Abs. 4 GG).

Spezialnetze der Verwaltung. Lokale Netze und IT-Systeme bei den Nutzern sowie über den IVÖV angebotene IT-Dienste sind dagegen nicht Bestandteil des IVÖV. Das Routing im gesamten IVÖV erfolgt in den Netzen und über die verbundenen Netze hinweg unter Anwendung von IPv6 gemäß IPv6-Adress- und Routingkonzept für die öffentliche Verwaltung[6]. Anbindungen zwischen den Netzen im IVÖV sowie an Drittnetze sind mittels abgesicherter Netzübergänge umgesetzt Im Rahmen der Gewährleistung der Mandantenfähigkeit im IVÖV sind in den verbundenen Netzen im IVÖV, in Abhängigkeit von Schutzbedarfen und (Nutzer-)Bedarfen, abgesicherte Netzzonen eingerichtet. Das Basisnetz im IVÖV wird auf Grundlage eines zentralen und redundant ausgelegten Backbone-Netzes im Kernbereich mit hoher Ausfallsicherheit betrieben. Es bildet die Plattform für den Anschluss von Netzen der öffentlichen Verwaltung von Bund, Ländern und Kommunen über den Anbindungsbereich im IVÖV.

Betriebsmodell
Im IVÖV richten die Nutzer auf Ebene Bund ihre IT-Bedarfe über das jeweils gültige Auftraggeber-/Auftragnehmer-Modell an die IT-Dienstleister des Bundes, während die Landes- bzw. Kommunalen IT-Dienstleister die Bedarfe der Nutzer auf Ebene der Länder und Kommunen erfüllen. Die IT-Dienstleister stellen den Nutzern in dieser Rolle IT-Dienste sowie die dafür erforderliche Konnektivität (i. S. v. Netzdienstleistungen) bereit. Letztgenannte beziehen diese von der BDBOS als zentrale Netzbetreiberin des Basisnetzes im IVÖV (gilt für Bund und Länder mit Opt-In Entscheidung) bzw. erbringen selbst die entsprechenden Netzdienstleistungen. Die BDBOS deckt den Großteil der für Netzdienstleistungen erforderlichen Funktionen in den Phasen Planung und Betrieb in Eigenbetrieb ab, während für den Aufbau ihr Schwerpunkt auf Spezifikation und Abnahme liegt.

Steuerung
Richtlinien und Standards sind mit Geltung für den gesamten IVÖV etabliert. Die Gremienstruktur und Rollenverteilung zur übergreifenden Steuerung und Abstimmung von Richtlinien und Standards für den IVÖV baut auf den gegenwärtig etablierten Strukturen auf: Der IT-Rat und die Konferenz der IT-Beauftragten steuern die Aktivitäten auf Ebene des Bundes. Der IT-Planungsrat mit dem Arbeitsgremium Verbindungsnetz koordiniert die Zusammenarbeit zwischen Bund und Ländern. Die Finanzierung der Bundesanteile am IVÖV orientiert sich am Nutzungsgrad der angeschlossenen Teilnehmer hinsichtlich der angebotenen Leistungen, während die Finanzierung des Verbindungsnetzes (im Anbindungsbereich) durch das IT-NetzG geregelt ist. Die Verantwortung für das Sicherheitsmanagement ist im IVÖV gemäß föderaler Zuständigkeit verteilt. Auf Ebene des Bundes und für Länder, welche das BSI mit der Absicherung der Ländernetze beauftragen (insbesondere Opt-In Länder), liegt diese zentral beim BSI.

Die zur Umsetzung des Zielbildes erforderlichen Maßnahmen werden dieser Netzstrategie nachgelagert in einem Umsetzungsdokument beschrieben. Das mehrdimensionale Zielsystem der Netzstrategie, die Herausforderungen bei der ebenenübergreifenden Zusammenarbeit von Bund, Ländern und Kommunen sowie der lange Umsetzungshorizont bis zum Jahr 2030 erfordern eine zentralisierte Steuerung und Koordination des Umsetzungsprogramms durch das Bundesministerium des Innern, für Bau und Heimat (BMI) in Absprache mit den betroffenen Bundesressorts. Zudem berichtet das BMI den Umsetzungsfortschritt an das Arbeitsgremium Verbindungsnetz des IT-Planungsrates sowie die auf Ebene des Bundes zuständigen Gremien. Die Aktualität der Netzstrategie sowie die regelmäßige Überprüfung des Fortschritts der Zielerreichung werden durch Etablierung eines Strategieprozesses, der nachgelagert zur Strategie konzipiert und abgestimmt wird, gewährleistet.

[6] Vgl. IT-Planungsrat (2016) Beschluss 2016/43 – IP-Adressverwaltung; Hinweis: Berücksichtigung IPv4-Strukturen im Rahmen der weitern Ausarbeitung des IPv6-Routingkonzepts erforderlich.

Inhaltsverzeichnis

1 Einführung

Die Digitalisierung der öffentlichen Verwaltung in Deutschland wirkt sich auf die digitale Zusammenarbeit sowohl innerhalb der Verwaltung als auch zwischen Verwaltung, Bürgerinnen und Bürgern, Wirtschaft und Wissenschaft sowie die im Rahmen dessen genutzten IT-Dienste und Fachverfahren[7] aus. Die weiterführende Entwicklung wurde in einer Vielzahl von Vorhaben des Koalitionsvertrages 2018 verankert. Fest geplant sind u. a. die Einführung der „vollständig elektronische[n] Vorgangsbearbeitung in der öffentlichen Verwaltung (E-Akte)“, das Fortführen der IT-Konsolidierung „mit großem Einsatz“, die Gestaltung des „Weg[es] in die Gigabit-Gesellschaft mit höchster Priorität“, die Einführung einer „nationale[n] Bildungsplattform“ und eines zentralen, digitalen Portals für Bürger und Unternehmen.[8]

Mit dieser Entwicklung steigt die Bedeutung des elektronischen Informationsaustausches sowie der digitalen Zugänge zu den Leistungen der Verwaltung (bspw. über den Portalverbund) für das Erreichen der Ziele und das Erfüllen der Aufgaben der öffentlichen Verwaltung. Immer wieder sind jedoch IT-Systeme und zugrundeliegende Netzinfrastrukturen der Verwaltung Angriffsziele von hochspezialisierten, professionellen Cyberattacken staatlicher und nichtstaatlicher Angreifer. Dies gilt in besonderem Maße auch für die Regierungskommunikation (i. S. v. vertraulicher Übermittlung von Informationen für die unmittelbare Regierungs- bzw. Kabinett-Arbeit), welche ein exponiertes Angriffsziel darstellt. Daher sind sichere und leistungsfähige Netzinfrastrukturen für die erfolgreiche Digitalisierung und die Aufgabenerfüllung der öffentlichen Verwaltung bereitzustellen.

Die Trends der Digitalisierung und Konsolidierung von IT finden sich ähnlich in den Bundesländern wieder, wobei sich die Herangehensweisen unterscheiden und die Heterogenität der Ansätze in Bezug auf die Kommunen eine spezifische Herausforderung darstellt.

Als weitere Herausforderungen sind die Heterogenität der Anforderungen an die Weitverkehrsnetze der öffentlichen Verwaltung, die Leistungserbringung für die Einrichtungen der öffentlichen Verwaltung in der Fläche, die gesetzlich föderal verteilten Zuständigkeiten, die technologische Komplexität, der Fachkräftemangel und die Zusammenarbeit der öffentlichen Verwaltung mit Dienstleistern zu nennen.

Es bedarf eines übergreifenden strategischen Ansatzes, um diesen Herausforderungen gemeinsam und konzertiert zu begegnen, sowie die Netzinfrastrukturen der öffentlichen Verwaltung abzusichern und weiterzuentwickeln. Die Bundesregierung legte im Jahr 2013 eine Gesamtstrategie IT-Netze der öffentlichen Verwaltung[9] zur strategischen Neuausrichtung der IT-Netze der öffentlichen Verwaltung vor. Seit dem Jahr 2013 wurden im Kontext der Netze richtungsweisende Grundsatzentscheidungen getroffen, und relevante Einflussfaktoren haben sich verändert. Zur Berücksichtigung und Begegnung dieser Einflussfaktoren gibt der Bund den Anstoß zur Fortschreibung der Gesamtstrategie in Form dieser Netzstrategie 2030 für die öffentliche Verwaltung.

Aufbau des Dokuments
In Kapitel 2 werden bestehende strategische Ansätze sowie ihr Umsetzungsstand und veränderte Rahmenbedingungen gewürdigt. In Kapitel 3 werden die Ziele und Handlungsfelder aus den Eckpunkte[n] einer Netzstrategie 2030 für die öffentliche Verwaltung[10] zusammengefasst. Diese wurden bei der Entwicklung dieser Netzstrategie auf Ebene des Bundes durch die Konferenz der IT-

[7] Begriffsbestimmung siehe Glossar Anhang B: Fachverfahren.

[8] Vgl. Koalitionsvertrag zwischen CDU, CSU und SPD für die 19. Legislaturperiode, 12. März 2018.

[9] Vgl. Bericht zur Gesamtstrategie der Netze der öffentlichen Verwaltung (2013).

[10] Der Beauftragte der Bundesregierung für Informationstechnik (2018): Eckpunkte einer Netzstrategie 2030 für die öffentliche Verwaltung.

Beauftragten der Ressorts (KoITB) beschlossen, Vertretern von Ländern und Kommunen vorgestellt sowie abschließend dem IT-Planungsrat zum Beschluss empfohlen[11]. Die Eckpunkte dienen als Rahmen für die Detaillierung der Netzstrategie 2030 für die öffentliche Verwaltung. Darauf aufbauend wird in Kapitel 4 das Zielbild 2030 für einen Informationsverbund der öffentlichen Verwaltung (IVÖV) beschrieben. Das Zielbild 2030 enthält Festlegungen und Optionen zur Gestaltung der Netze der öffentlichen Verwaltung sowie der gemeinsamen Nutzung von Infrastrukturen und Fähigkeiten des Betriebs und der Absicherung. Es stellt für den Bund eine grundsätzlich verbindliche Planung dar, während es für die Länder (und Kommunen) Optionen aufzeigt.

Auf Grundlage des Zielbildes 2030 gibt Kapitel 5 einen Ausblick, wie strategische Maßnahmen zur Umsetzung dieser Netzstrategie, d. h. zur Erfüllung des Zielbildes 2030, zu beschreiben und in Form eines Umsetzungsdokuments zusammenzustellen sind. Darüber hinaus wird zur Gewährleistung der Aktualität der Netzstrategie sowie zur Bewertung der Zielerreichung einzelner Maßnahmen durch das BMI in Abstimmung mit dem IT-Controlling Bund ein Strategieprozess entwickelt. Bis zum Jahr 2030 sind Änderungen grundlegender Rahmenbedingungen möglich. Diese werden im Rahmen des Strategieprozesses bei der Aktualisierung der Strategie berücksichtigt.

[11] IT-Planungsrat (2018), Entscheidung 2018/52; Der IT-Planungsrat hat die Eckpunkte einer Netzstrategie 2030 in der 27. Sitzung am 25.10.2018 zur Kenntnis genommen. Die Zusammenarbeit von Bund, Ländern und Kommunen bei der weiteren Detaillierung der Strategie ist fortzuführen.

2 Umsetzungsstand bestehender Ansätze und veränderte Rahmenbedingungen

Mit dem Leitbild aus der Gesamtstrategie IT-Netze der öffentlichen Verwaltung[12] wurden 2013 Festlegungen für die strategische Neuausrichtung und langfristige Weiterentwicklung der Weitverkehrsnetze der öffentlichen Verwaltung vorgegeben. Darauf aufbauend wurden seitdem Grundsatzentscheidungen gefasst und Vorhaben initiiert, deren Umsetzungsstände im Folgenden zusammengefasst werden. Darüber hinaus werden zentrale veränderte Einflussfaktoren skizziert, die eine Fortschreibung der Strategie mit einer übergreifenden Ambition für Bund und Länder erforderlich machen.

2.1 Leitbild der Gesamtstrategie IT-Netze der öffentlichen Verwaltung (2013)

Der Ansatz einer Gesamtstrategie IT-Netze der öffentlichen Verwaltung[13] von 2013 war insbesondere durch die wachsende Bedeutung bund-/länderübergreifender Zusammenarbeit bei IT-basierten Fachverfahren in der öffentlichen Verwaltung (bspw. Umsetzung IT-NetzG) sowie durch die verschärfte Cyberbedrohungslage motiviert. Um diesen Herausforderungen zu begegnen, legte die Gesamtstrategie folgendes zentrale Leitbild für sicherheitskritische IT-Systeme und IT-Infrastrukturen des Bundes fest:

> *„Der Bund muss seine sicherheitskritischen IT-Systeme und Infrastrukturen soweit wie möglich selbst planen, aufbauen und betreiben. Dort, wo dieses nicht möglich ist, muss er zumindest die Kontrolle hierüber haben."*[14]

Dieses Leitbild formuliert die Ambition des Bundes, die Souveränität über seine sicherheitskritischen IT-Systeme und Infrastrukturen durch eine hohe Fertigungstiefe im Bereich der Netze (als Teil der IT-Infrastrukturen) zu gewährleisten.

2.2 Umsetzungsstand Gesamtstrategie IT-Netze der öffentlichen Verwaltung

Gemäß Gesamtstrategie von 2013 bildet NdB die Grundlage für die aufzubauenden strategischen Kompetenzen innerhalb der Bundes-, Länder- und Kommunalverwaltungen. Dem Leitbild der Gesamtstrategie folgend, werden weitere Vorhaben im Kontext der Netze geplant und umgesetzt: Dazu zählen die Auswahl der BDBOS als bundeseigene Betreiberin für die konsolidierten Netze der Bundesverwaltung (bzw. der Integrationsplattform NdB 1.0) und die Vorbereitung weiterer Konsolidierungen (NdB ab 2019). Darüber hinaus wurde im Rahmen des Projektes NdB festgelegt, das Kerntransportnetz Bund (KTN-Bund) als Backbone-Netz für die Netze der Bundesverwaltung zu nutzen.

Umsetzungsstand Projekt NdB
Mit dem Projekt NdB werden die Grundlagen für ein gemeinsames Netz der Bundesverwaltung zur sicheren Kommunikation geschaffen. Dazu wurden durch das Projekt die vom BMI verantworteten

[12] Vgl. Bericht zur Gesamtstrategie der Netze der öffentlichen Verwaltung (2013).

[13] Vgl. Bericht zur Gesamtstrategie der Netze der öffentlichen Verwaltung (2013).

[14] Vgl. Bericht zur Gesamtstrategie der Netze der öffentlichen Verwaltung (2013).

ressortübergreifenden Bestandsnetze der Bundesverwaltung Informationsverbund Berlin-Bonn (IVBB), das Bundesverwaltungsnetz (BVN) sowie die Deutschland Online Infrastruktur (ehemals DOI, heute NdB-Verbindungsnetz) vollständig auf NdB als Integrationsplattform migriert und somit konsolidiert. NdB soll auf dem Kerntransportnetz-Bund (KTN-Bund) aufbauen, wobei hiermit keine langfristige Festlegung für das KTN-Bund auf einen Provider erfolgen soll.[15] Neben diversen Herausforderungen bei der Umsetzung machte insbesondere die einheitlich festgelegte (nicht bedarfsgerechte) Schutzzone für bestimmte IT-Dienste bereits während des Projektes die Konzeption und den Aufbau eines NdB-Extranets erforderlich („IT-Grundschutznetz"). Dieses berücksichtigt besondere Anforderungen an die Kommunikation mit nationalen und internationalen Partnern aus Wirtschaft, Wissenschaft und Gesellschaft. Das Projekt wurde 2015 begonnen und wird voraussichtlich mit dem Übergang der Betriebsverantwortung zur BDBOS als zentrale Betriebsorganisation am 1. Januar 2019 abgeschlossen.

Auswahl und Aufbau einer Betriebsorganisation für den Betrieb von NdB
Im Mai 2016 forderte der Haushaltsausschuss des Deutschen Bundestages (HHA) von der Bundesregierung eine Empfehlung zur Festlegung einer geeigneten staatlichen Betriebsorganisation für NdB. Die Betriebsübernahme durch die Organisationen Informationstechnikzentrum Bund (ITZBund), BWI sowie BDBOS wurden als Optionen bewertet. Im Ergebnis wurde empfohlen, die BDBOS ab dem Jahr 2019 mit der Betriebsübernahme und der Weiterentwicklung von NdB zu beauftragen, da bei der BDBOS die Strukturen und Erfahrungen für den Betrieb des KTN-Bund (Layer 2-Netz) bereits existieren und die Kriterien für eine Betriebsorganisation unter Kontrolle des Bundes erfüllt sind. Es ist geplant, dass die BDBOS ab 2019 bis zum Jahr 2020/2021 die Transition zu einem weitgehend eigenständigen Regelbetrieb von NdB abschließt. Der Anteil der durch die BDBOS geleisteten Betriebsaufgaben wird über diesen Zeitraum kontinuierlich erhöht und ist hauptsächlich durch die Rate der Personalgewinnung begrenzt.

Planungsstand Projekt NdB ab 2019
Die ursprüngliche Planung sah vor, dass das im Projekt NdB errichtete Netz (NdB 1.0) als Integrationsplattform zur Konsolidierung[16] weiterer Weitverkehrsnetze der Bundesverwaltung dienen wird. In diesem Zusammenhang wurde die Bundesregierung durch den Beschluss des HHA[17] aufgefordert, das Architekturboard als Steuerungsgremium einzurichten. Vertreter der Ressorts BMI, BMF, BMVI und BMVg sowie der BDBOS (nicht stimmberechtigt) und des BSI sind mit der Abstimmung und Migrationsplanung für weitere Netze auf die mit NdB 1.0 geschaffene Integrationsplattform im Zuständigkeitsbereich der genannten Ressorts beauftragt.[18] Seit 2018 ist auch das Auswärtige Amt (AA) Mitglied des Architekturboards; eine Migration insbesondere des internationalen Netzes der Auslands-IT auf NdB ist zum heutigen Zeitpunkt allerdings nicht vorgesehen.[19] Die Migrationsplanung für den Zeitraum ab 2019 befindet sich gegenwärtig in Erarbeitung unter Federführung des BMI (aktuell: Referat BMI CI 5) in Abstimmung mit dem Architekturboard. Zur Festlegung der im nächsten Schritt zu migrierenden bzw. konsolidierenden Weitverkehrsnetze müssen die langfristig zu nutzenden Backbone-Netze und die Aufgabenverteilung gegenüber den zentralen IT-Dienstleistern des Bundes festgelegt werden, um Übergangsphasen zu vermeiden bzw. deren

[15] Beschluss der 29. Sitzung des Haushaltsauschusses am 12. November 2014.

[16] Begriffsbestimmung siehe Glossar Anhang B: Konsolidierung.

[17] Haushaltsausschuss (2014).

[18] Siehe BDBOS (2016) für weitere Details und Erläuterungen.

[19] Aufgrund der besonderen Anforderungen des Auswärtigen Amtes an die Kommunikation insbesondere mit deutschen Dienststellen im Ausland und internationalen Partnern sowie dem speziellen Charakter des weit verzweigten Netzes im In- und Ausland ist eine vollständige Migration auf NdB weder möglich (nationale Begrenzung des KTN-Bund) noch vorgesehen.

Dauer zu reduzieren. Zu diesem Zweck wird auch geprüft, die o. g. Backbone-Netze in die technische Architektur des IVÖV zu migrieren.

Erwerbsoption Leerrohrinfrastruktur
Für den angestrebten Ausbau der Fertigungstiefe des Bundes im Bereich Netze wurde der Erwerb einer dem Bund angebotenen Leerrohrinfrastruktur durch das BMI geprüft. Nach einer monetären Wirtschaftlichkeitsbetrachtung und Bewertung sicherheitstechnischer Implikationen wurde der Erwerb abgelehnt.

2.3 Veränderte Rahmenbedingungen

Seit Beschluss der Gesamtstrategie 2013 haben sich Rahmenbedingungen verändert, die direkten oder indirekten Einfluss auf die Netze der öffentlichen Verwaltung haben. Zu diesen Rahmenbedingungen gehören bspw. die Konzepte und der Fortschritt der IT-Konsolidierung Bund, die verpflichtenden Mindestanforderungen der Cybersicherheitsstrategie für Deutschland 2016 sowie des Umsetzungsplans Bund 2017 und die Zusammenarbeit von Bund und Ländern – und damit auch die Interoperabilität deren IT - zur Umsetzung des Onlinezugangsgesetzes.

IT-Konsolidierung des Bundes
Im Zuge der drei Handlungsstränge der IT-Konsolidierung (Betriebs-, Beschaffungs- und Dienstekonsolidierung) wird die IT-Leistungserbringung der Bundesverwaltung gebündelt und ein Leistungsverbund der IT-Dienstleister des Bundes etabliert. Zu diesem zählen BWI, ITZBund sowie die Auslands-IT des Auswärtigen Amtes, das BA-IT-Systemhaus und die IT des DRV Bund. Des Weiteren ist die zentrale Netzbetreiberin BDBOS ebenso dem IT-Leistungsverbund zuzuordnen. Im Rahmen der Dienstekonsolidierung, bspw. durch den Aufbau einer Bundescloud, werden weitere Bündelungs- und Konsolidierungseffekte durch Zentralisierung der IT-Leistungserbringung angestrebt. Diese Entwicklungen sind Treiber eines stark veränderten Anforderungsprofils in Bezug auf die Leistungsfähigkeit, Sicherheit und Verfügbarkeit der zugrundeliegenden Netzinfrastrukturen. Der fortschreitende Verlauf der IT-Konsolidierung Bund hat somit weitreichende Folgen für die Anforderungen an die Leistungsfähigkeit der Netze der Bundesverwaltung. Unter anderem wird aufgrund der Betriebskonsolidierung der Datenverkehr in den Weitverkehrsnetzen erhöht, wodurch deren Kritikalität für die Handlungsfähigkeit der öffentlichen Verwaltung hinsichtlich der Kommunikation steigt. Dementsprechend ist eine enge Abstimmung zwischen der IT-Konsolidierung Bund und den Vorhaben zur Konsolidierung der Weitverkehrsnetze der Bundesverwaltung notwendig.

Umsetzungsplan Bund 2017
Der Schutz des deutschen Anteils am Cyberraum und das Vorhandensein möglichst widerstandsfähiger Infrastrukturen, sind wesentliche Ziele deutscher Politik. Die Cybersicherheitsstrategie für Deutschland 2016 bildet den ressortübergreifenden strategischen Rahmen für die Aktivitäten der Bundesregierung mit Bezug zur Cybersicherheit. Auf deren Grundlage wurde mit dem Umsetzungsplan Bund 2017 (UP Bund)[20] eine Informationssicherheitsstrategie auf Ebene des Bundes entwickelt. Der UP Bund stellt die Informationssicherheitsleitlinie des Bundes dar und definiert die verbindlichen Rahmenbedingungen für den Schutz der in der Bundesverwaltung verarbeiteten Informationen und der dabei genutzten IT-Systeme, Dienste und Kommunikationsnetzinfrastrukturen. Im Fokus steht dabei die Etablierung und Aufrechterhaltung von Prozessen zur mittel- und langfristigen Gewährleistung der Informationssicherheit in der Bundesverwaltung. Der UP Bund fokussiert somit die Schutzziele der Informationssicherheit - Vertraulichkeit, Verfügbarkeit und Integrität - der in der Bundesverwaltung erhobenen, verarbeiteten und genutzten Informationen. Die Regelungen des UP Bund gelten für alle Ressorts und Bundesbehörden und sind im jeweiligen

[20] Vgl. Bundesministerium des Innern (2017).

Zuständigkeitsbereich eigenverantwortlich durchzusetzen. Die Festlegungen in diesem Umsetzungsplan sind als verbindliche und einheitliche Mindestanforderungen zu verstehen.

Anstoß für die Fortschreibung des Umsetzungsplans für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung aus dem Jahre 2007 waren geänderte Rahmenbedingungen im Bereich der IT der öffentlichen Verwaltung, u. a. die fortschreitende Digitalisierung der Verwaltung, Verschärfung der IT-Sicherheitslage, neue Regelungen im Bereich Cybersicherheit sowie die Konsolidierung der IT des Bundes. Der Umsetzungsplan Bund 2017 gibt u. a. Hinweise zu Informationssicherheitsmanagementsystemen (ISMS), Personalentwicklung im Bereich Sicherheitsmanagement, kritischen Geschäftsprozessen, Informationssicherheitsanforderungen an Dienstleister und Dienstleistungen sowie IT-Notfallprävention und IT-Krisenreaktion.

Cybersicherheitslage und gemeinsame Ansätze von Bund und Ländern
Zu den maßgeblichen Einflüssen auf die Digitalisierung der Verwaltung zählt die Cybersicherheitslage, gekennzeichnet durch die stark ansteigende Professionalisierung von gezielten Cyberangriffen staatlicher und nichtstaatlicher Organisationen auf Systeme und Infrastrukturen der öffentlichen Verwaltung sowie der deutschen Wirtschaft. Die Folgen von Cyberangriffen sind nicht auf den Cyberraum beschränkt, sondern können gesellschaftliche, wirtschaftliche sowie politische Schäden verursachen. Angriffe auf staatliche Institutionen mit dem Ziel der Ausspähung oder Sabotage beeinträchtigen die Funktionsfähigkeit der Verwaltung und haben somit erhebliche Auswirkungen auf die öffentliche Sicherheit und Ordnung in Deutschland.

Um eine rasche, ganzheitliche Sicherung der Systeme und Infrastrukturen für alle Ebenen der öffentlichen Verwaltung zu gewährleisten, wird die Zusammenarbeit von Bund und Ländern durch die Cybersicherheitsstrategie für Deutschland[21] gestärkt. Daraus geht hervor, dass das BSI perspektivisch auch Landesbehörden unterstützen wird, soweit diese mit der Bewältigung von Cybersicherheitsvorfällen befasst sind. Die Zusammenarbeit schließt u. a. die Festlegung allgemeiner Maßstäbe für die föderale IT-Sicherheit zur gemeinsamen Abwehr von Cyberangriffen sowie die verbindliche Regelung des bislang freiwilligen Austausches zwischen Bund und Ländern von Informationen zu IT-Sicherheitsvorfällen ein. Darüber hinaus wird angestrebt, die Cybersicherheit durch Etablierung eines einheitlichen und einvernehmlichen Mindestsicherheitsniveaus unter Berücksichtigung des Grundsatzes der Wirtschaftlichkeit[22] gemäß der durch den IT-Planungsrat verabschiedeten Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung[23] zu erhöhen. Dementsprechend wird Fachwissen der Bundesbehörden über die Länder auch Kommunen zur Verfügung gestellt.[24]

Trotz der Verabschiedung gemeinsamer Grundsätze für die ebenenübergreifende Absicherung und Zusammenarbeit, stellt die starke Heterogenität der Netzlandschaft der öffentlichen Verwaltung eine besondere Herausforderung dar, weshalb eine weitere Konkretisierung der Konzepte (bspw. Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung) für Länder und Kommunen erforderlich ist.

Einordnung Netze der Landes- und Kommunalverwaltungen
Die Verbindung zwischen Bund und Ländern (u. a. IVBB) wurde zunächst mit Hilfe der Deutschland Online-Infrastruktur (DOI) realisiert und später im Rahmen des Projektes NdB 1.0 auf die Integrati-

[21] Bundesministerium des Innern (2016): Cyber-Sicherheitsstrategie für Deutschland; Es ist zu prüfen, ob diese zusätzlichen Aufgaben des BSI hinsichtlich der Zusammenarbeit mit den Ländern auch im BSI-Gesetz verankert werden sollten.

[22] Der Grundsatz der Wirtschaftlichkeit und Sparsamkeit gemäß § 7 BHO muss auch im Kontext der Fortentwicklung der Informationssicherheit gewahrt bleiben.

[23] Vgl. IT-Planungsrat (2013), Beschluss 2013/01: Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung.

[24] Vgl. Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen.

onsplattform NdB migriert. Das DOI-Netz bzw. das NdB-Verbindungsnetz fungier(t)en somit als Verbindungsnetz gemäß IT-NetzG.

Unabhängig von den Netzen der Bundesverwaltung werden Ländernetze im Verantwortungsbereich der jeweiligen Länder betrieben. Die Ländernetze sind heterogen und unterscheiden sich stark, u. a. mit Blick auf die gewählten Betreibermodelle, umgesetzte Fertigungstiefen, Sicherheitsniveaus und Krisenfestigkeit. Auch die Konsolidierung einzelner Netze ist in den Ländern unterschiedlich weit fortgeschritten. So ist bspw. der Netzbetrieb mehrerer Ländernetze bei einem IT-Dienstleister mit hoher eigener Fertigungstiefe unter Steuerung der öffentlichen Hand gebündelt. Des Weiteren verlangt die aktuelle Gesetzeslage mit dem Onlinezugangsgesetz eine starke, übergreifende Zusammenarbeit von Bund, Ländern und Kommunen; folglich auch deren IT-Dienstleistern. Die Wahrung der Hoheit von Bund und Ländern muss jedoch bei der Konzeption übergreifender Zusammenarbeitsmodelle berücksichtigt bzw. die aktuell geltenden Rahmenbedingungen einvernehmlich modernisiert werden.

Mangelnde Abstimmung, das Fehlen gemeinsamer Standards und Herangehensweisen innerhalb und zwischen den Ländernetzen hemmt bisher Interoperabilität in der öffentlichen Verwaltung, welche mit Blick auf gestiegene und zukünftig noch weiter steigende Kommunikationsanforderungen zu gewährleisten ist. Die angestoßenen Projekte NdB, IT-Konsolidierung Bund sowie Maßnahmen zur Abwehr von Cyberangriffen stellen jeweils wichtige Faktoren zur Bewältigung der Herausforderungen der digitalen Verwaltung dar. Um die Effekte der Maßnahmen zu kanalisieren und zu verstärken, wird perspektivisch eine einheitliche Koordination der bisher größtenteils unabhängigen Vorhaben erforderlich.

Mit einem Informationsverbund der öffentlichen Verwaltung auf Ebene des Bundes mit Angeboten an die Länder wird ein übergreifendes Konzept zur Weiterentwicklung der Netzlandschaft für Bund und Länder initiiert.

3 Eckpunkte einer Netzstrategie für die öffentliche Verwaltung

Um den strategischen Herausforderungen für die Entwicklung der Weitverkehrsnetze der öffentlichen Verwaltung zu begegnen, wurden Eckpunkte einer Netzstrategie definiert und auf Ebene des Bundes am 25.06.2018 durch die Konferenz der IT-Beauftragten der Ressorts (KoITB) beschlossen.[25] Des Weiteren wurden die Eckpunkte Vertretern von Ländern und Kommunen vorgestellt sowie abschließend dem IT-Planungsrat zum Beschluss empfohlen.[26] Ausgehend von Herausforderungen, Prämissen und Rahmenbedingungen sowie Anforderungen an die Netzstrategie, zeigen die Eckpunkte strategische Ziele und Handlungsfelder der Netzstrategie auf und beschreiben Grundlagen für das in Kapitel 4 dargestellte Zielbild 2030.

3.1 Strategische Ziele

Das übergeordnete Ziel für die Weitverkehrsnetze der öffentlichen Verwaltung Deutschlands ist die Gewährleistung bedarfsgerechter und sicherer Kommunikation zwischen den Einrichtungen der öffentlichen Verwaltung. Dieses Ziel ist u. a. motiviert durch die zunehmend erforderlichen Kommunikationsbeziehungen im Rahmen der Umsetzung des Onlinezugangsgesetzes sowie (bundesseitig) der IT-Konsolidierung Bund und vor dem Hintergrund einer insgesamt heterogenen und in Teilen fragmentierten Betreiber- und Netzstruktur und der Entwicklung der Cybersicherheitslage. Diese und weitere Einflussfaktoren sowie Herausforderungen für die Netze der öffentlichen Verwaltung wurden in den Eckpunkten der Netzstrategie ausführlich dargelegt. Die in den Eckpunkten festgelegten Ziele lauten:

- **Leistungsfähigkeit:** Heutige und zukünftige Anforderungen an Bandbreite, Latenz, Quality of Service, nutzbare Dienste/ Protokolle, Resilienz und Handlungsfähigkeit in besonderen Lagen werden bedarfsgerecht erfüllt.
- **Digitale Zusammenarbeit von Bund und Ländern:** Netzinfrastrukturen der öffentlichen Verwaltung erlauben die digitale und ebenenübergreifende Zusammenarbeit zwischen Nutzern von Bund, Ländern/Kommunen sowie Partnern in anderen Staaten, Institutionen im Ausland, bspw. aus Partnerstaaten der Europäischen Union[27] und Staaten im Kontext der wirtschaftlichen Zusammenarbeit und Entwicklung. Sie dienen der (teilweise) gesetzlich geforderten, aber auch gesellschaftlich gewollten Kommunikation mit den Bürgerinnen und Bürgern, der Wirtschaft und der Wissenschaft.
- **Informationssicherheit:** Die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen ist für die Kommunikation der öffentlichen Verwaltung auch in besonderen Lagen von eminenter Bedeutung. Ziel ist die Sicherstellung einer mit dem BSI einvernehmlich gestalteten Sicherheitsarchitektur um u. a. professionellen Angriffen präventiv und reaktiv zu begegnen. Dazu sollen BSI-geprüfte Produkte/Entwicklungen Verwendung finden. Die IVÖV-Architektur kann bei Bedarf unter Einhaltung gewisser Rahmenbedingungen flexibel angepasst werden.

[25] Der Beauftragte der Bundesregierung für Informationstechnik (2018): Eckpunkte einer Netzstrategie 2030 für die öffentliche Verwaltung.

[26] IT-Planungsrat (2018), Entscheidung 2018/52; Der IT-Planungsrat hat die Eckpunkte einer Netzstrategie 2030 in der 27. Sitzung am 25.10.2018 zur Kenntnis genommen.

[27] Als Beispiele im Justizbereich sind Eurojust und ECRIS zu nennen.

- **Datenschutz:** Der Datenschutz in den Netzinfrastrukturen der öffentlichen Verwaltung wird durch wirksame Maßnahmen gemäß Art. 25 und 32 EU-Datenschutz-Grundverordnung gewährleistet.
- **Nationale digitale Souveränität:** Die öffentliche Verwaltung verfolgt für den IVÖV ein Eigenbetriebsmodell durch einen internen Netzdienstleister. Sie sichert sich hiermit Kontroll-, Durchsetzungs- und Wahlmöglichkeiten bei Planung, Aufbau und Betrieb von Netzinfrastrukturen. Dies umfasst auch Beschaffung von Produkten und Dienstleistungen sowie Vorgaben zur Übertragung von Daten ausschließlich innerhalb deutscher Landesgrenzen (nationales Routing).[28] Der Bund wird seiner besonderen Verantwortung in Krisensituationen gerecht. Der Abwanderung von Entwicklern/Herstellern von erforderlichen Schlüsseltechnologien wird entgegengewirkt.
- **Zukunftsfähigkeit und Flexibilität:** Die Gestaltung der Netzinfrastrukturen der öffentlichen Verwaltung erlaubt den flexiblen Einsatz neuer – möglichst standardisierter – Technologien und die bedarfsgerechte Ausweitung der Nutzergruppen mit unterschiedlichen Anforderungen.
- **Wirtschaftlichkeit:** Planung, Aufbau und Betrieb der Netzinfrastrukturen der öffentlichen Verwaltung erfolgen bei festgelegtem Leistungsumfang wirtschaftlich.

3.2 Strategische Handlungsfelder

Für die Erreichung der Ziele wurden sechs strategische Handlungsfelder definiert:

- **Strategische Ausgestaltung der Fertigungstiefe**
  Der Bund gestaltet seine Fertigungstiefe bei Netzinfrastrukturen aktiv und strategisch zur Wahrung einer nationalen digitalen Souveränität im Sinne der Beherrschbarkeit der Netze. Für Planung, Aufbau und Betrieb entwickeln Bund und Länder eigene Fähigkeiten zielgerichtet weiter und stellen sich diese gegenseitig und bei Bedarf weiteren Kooperationspartnern bereit. Abhängigkeiten von wenigen externen Dienstleistern werden reduziert. Dennoch ist es wirtschaftlich sinnvoll, hinsichtlich Ausbau, Wartung und Reparatur Wahlmöglichkeiten zwischen als verlässlich kategorisierten externen Dienstleistern gezielt aufzubauen.
- **Weiterentwicklung aktiver Dienstleistersteuerung**
  Der Bund entwickelt Managementprozesse zur Steuerung seiner internen und externen Dienstleister für Planung, Aufbau und Betrieb von Netzinfrastrukturen weiter. Es findet ein Austausch der gewonnenen Erkenntnisse und Best Practices mit den Ländern statt. Umfassende Transparenz zu eingesetzten Technologien über die gesamte Lieferkette wird über einen etablierten strukturierten und wiederkehrenden Prozess hergestellt.
- **Konsolidierung von Weitverkehrsnetzen und Standardisierung**
  Durch Konsolidierung seiner Weitverkehrsnetze in einen Informationsverbund schafft der Bund inklusive des Verbindungsnetzes eine Integrationsplattform primär für die Anbindung der gesamten öffentlichen Verwaltung über die jeweiligen Weitverkehrsnetze. In Abstimmung mit den Ländern definiert der Bund verbindliche Standards für den Bereich Netze sowie deren Informations- und Datensicherheit mit bedarfsgerechten Ausprägungen un-

[28] Eine Ausnahme gilt für Dienststellen, die aus besonderen Gründen unmittelbar jenseits der deutschen Grenze angesiedelt sind (gemeinsame Grenzdienststellen, Grenzzollämter u. ä.).

ter Wahrung von Flexibilität (bspw. für Ressortforschungseinrichtungen). Der Bund ergreift Maßnahmen zur Durchsetzung dieser Standards.

- **Gewährleistung Informationssicherheit und Datenschutz in Netzinfrastrukturen der öffentlichen Verwaltung**
  Der IVÖV verbindet Nutzer auf Bundes-, Landes- und Kommunalebene und schafft den Bürgerinnen und Bürgern sowie der Wirtschaft Zugänge zu den Online-Diensten der öffentlichen Verwaltung unter Sicherung von Verfügbarkeit, Integrität und Vertraulichkeit. Die Kommunikationsfähigkeit mit internationalen Partnern (bspw. EU) wird durch einheitliche, zentral geregelte Netzübergänge sichergestellt. Im IVÖV werden Bedarfe der Nutzer an Sicherheit in einem geordneten Prozess identifiziert und Sicherheitsniveaus bedarfsgerecht bereitgestellt (sog. „Zwiebelschalenmodell“[29] mit Kommunikationsmöglichkeit außerhalb der VS-Stufen).

- **Weiterentwicklung des Anforderungs- und Nutzermanagements**
  Im IVÖV werden (Nutzer-)Anforderungen konsequent und über alle Ebenen gebündelt und bei der Weiterentwicklung und Steuerung des Serviceangebotes der Netzinfrastrukturen der öffentlichen Verwaltung berücksichtigt. Das Serviceangebot wird mit Blick auf Leistungsumfang (Bandbreite, Quality of Service etc.) sowie Sicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) abgestuft. Änderungen am Serviceangebot und damit verbundenen Abläufen sowie Anfragen und Vorfälle werden über definierte Prozesse kommuniziert.

- **Förderung von Innovationen und Schlüsseltechnologien für eine bürgernahe und moderne Verwaltung**
  Die öffentliche Verwaltung fördert Innovationen im Bereich Netzwerk- und Sicherheitstechnologien (i. S. v. Forschungs- und Wirtschaftsförderung sowie Förderung von Clustern). Innovative Entwicklungen werden aufgegriffen und in den Netzen der öffentlichen Verwaltung eingesetzt. Der Bund etabliert einen Regelprozess zur Identifikation und Bewertung von Innovationen. Ergebnisse werden mit den Ländern fortlaufend abgestimmt. Für die flächendeckende Nutzung von Innovationen wird eine leistungsfähige Integrationsplattform bereitgestellt.

[29] Mit dem Zwiebelschalenmodell wird allgemein die Modularität des Angebots von Leistungen im IVÖV beschrieben. Im Zusammenhang verschiedener Sicherheitsniveaus ist damit die variable, modulare Auswahl von Sicherheitsniveaus von offen bis VS-Geheim referenziert.

4 Zielbild 2030 für einen Informationsverbund der öffentlichen Verwaltung

Das im Folgenden dargestellte Zielbild 2030 beschreibt den angestrebten Zielzustand im Jahr 2030 für den Informationsverbund der öffentlichen Verwaltung (IVÖV) und der zugrundeliegenden Weitverkehrsnetze der öffentlichen Verwaltung. Diese dienen den Einrichtungen der Verwaltung des Bundes, der Länder und Kommunen und ermöglichen auch Kommunikation mit Partnern im Ausland, mit Staaten im Kontext der wirtschaftlichen Zusammenarbeit und Entwicklung sowie mit der Wirtschaft und den Bürgerinnen und Bürgern (z. B. im Rahmen der Verwaltungsdigitalisierung gemäß Onlinezugangsgesetz). Die Gestaltung des Zielbilds 2030 folgt den in der Einleitung gewürdigten Grundsatzentscheidungen (siehe Kapitel 2) zur Entwicklung von NdB als Integrationsplattform für die Weitverkehrsnetze der Bundesverwaltung, für die Ertüchtigung der BDBOS als Betreiberin dieser Integrationsplattform, zur Nutzung des KTN-Bund als Backbone-Netz für die Integrationsplattform sowie den dieser Netzstrategie zugrundeliegenden Eckpunkten.[30] Dieses Zielbild 2030 beschreibt im Hinblick auf die Weitverkehrsnetze der öffentlichen Verwaltung die Technische Architektur, das Betriebsmodell, die Steuerung und erläutert Definition und Gegenstand des IVÖV. Der beschriebene Informationsverbund der öffentlichen Verwaltung stellt einen Rahmen für die Entwicklung der Weitverkehrsnetze der öffentlichen Verwaltung dar, innerhalb welchem Standards und Richtlinien abgestimmt werden sollen. Die Regelungen zur Verbindung der informationstechnischen Netze des Bundes und der Länder über das Verbindungsnetz nach dem IT-NetzG bzw. Art. 91 c GG bleiben davon unberührt. Die Maßnahmen zur Umsetzung des Zielbildes 2030 im Rahmen einer strategischen Roadmap sind in einem separaten Umsetzungsdokument zu beschreiben. Während das Zielbild für die Bundesverwaltung nach Festlegung der konkreten Maßnahmen verbindlich umzusetzen ist, stellen die im Zielbild beschriebenen Netzdienstleistungen ein Angebot für die Verwaltung der Länder (und Kommunen) dar, über deren Nutzung die Länder (bzw. Kommunen) eigenständig entscheiden. Demzufolge beziehen sich alle Regelungen der Netzstrategie zunächst ausschließlich auf Weitverkehrsnetze in Verantwortung des Bundes.[31] Mit Blick auf die Umsetzbarkeit des Zielbildes wird in der Netzstrategie bereits zwischen der Verantwortlichkeit (i. S. d. Erfolgsverantwortung) sowie der Zuständigkeit für die Umsetzung (i. S. v. tatsächlichen Aktivitäten) unterschieden.

4.1 Definition Informationsverbund der öffentlichen Verwaltung

Aus Sicht der Einrichtungen der öffentlichen Verwaltung (fachliche Sicht) ist der IVÖV ein Netzverbund zwischen Nutzern (i. S. v. Einrichtungen) und Anbietern (i. s. V. Betreibern) von IT-Diensten (i. S. v. Anwendungen und Fachverfahren) und dient der Kommunikation der öffentlichen Verwaltung von Bund, Ländern und Kommunen sowie mit (inter-)nationalen Partner aus Wirtschaft, Wissenschaft und Verwaltung bzw. Bürgerinnen und Bürgern. Die Gesamtheit infrastruktureller, organisatorischer, personeller und technischer Bestandteile von Weitverkehrsnetzen zur Bereitstellung

[30] Der Beauftragte der Bundesregierung für Informationstechnik (2018): Eckpunkte einer Netzstrategie 2030 für die öffentliche Verwaltung.

[31] Für Länder und Kommunen besteht die Möglichkeit, die BDBOS als Bundesbehörde mit dem Betrieb des Ländernetzes zu beauftragen. In diesem Falle befinden sich die entsprechenden Netze auch in Verantwortung des Bundes. Insgesamt können die Länder die angebotenen Leistungen im IVÖV freiwillig und modular nutzen. So ist es bspw. für Länder möglich, unabhängig von der Wahl des Betreibermodells das BSI mit dem Management der Informationssicherheit (vgl. Kapitel 4.1.2, Security as a Service) in ihren Netzen zu beauftragen.

von Netzdienstleistungen[32] sind zentrale Komponenten des IVÖV. Der IVÖV umfasst somit die verbundenen Netze der Bundesverwaltung und Netze der Auslands-IT des Auswärtigen Amtes, das Verbindungsnetz gem. IT-NetzG[33], die verbundenen Netze von Landes- und Kommunalverwaltungen sowie ggf. weitere Spezialnetze der Verwaltung. Lokale Netze und IT-Systeme (Clients, Server, etc.) bei den Nutzern sowie über den IVÖV angebotene IT-Dienste (i. S. v. Anwendungen und Fachverfahren) sind dagegen nicht Bestandteil des IVÖV.

Über den IVÖV stellen die IT-Dienstleister den Nutzern IT-Dienste bereit. Im Kontext des IVÖV nehmen sowohl Nutzer der IT-Dienste als auch IT-Dienstleister (als Anbieter von IT-Diensten) die im IVÖV angebotenen Netzdienstleistungen in Anspruch (siehe Kapitel 4.1.1.).[34] Die Grundlage dafür bilden die von der BDBOS als zentrale Betreiberin des Basisnetzes im IVÖV verantworteten netznahen Dienste[35]. Zusätzlich werden Nutzern (i. S. v. Einrichtungen) weitere Netz- bzw. Sicherheitsbezogene Dienstleistungen angeboten. Das Angebot umfasst dabei auch die Möglichkeit, die BDBOS mit dem Betrieb eines Landesnetzes zu beauftragen (Opt-In Entscheidung). Abbildung 1 skizziert illustrativ die Nutzer und Anbieter im IVÖV.

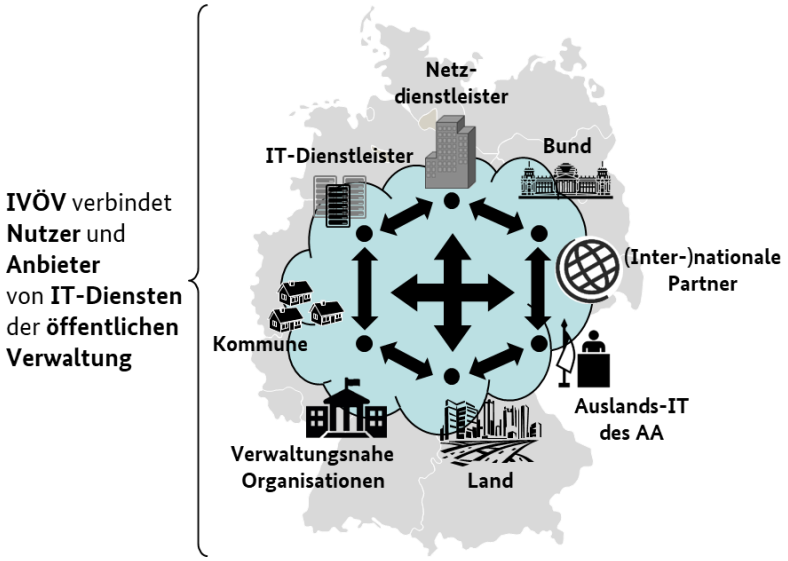


Abbildung 1: Fachliche Sicht - Informationsverbund der öffentlichen Verwaltung

4.1.1 Nutzergruppen des IVÖV

Aus einer fachlichen Sicht (vgl. Abbildung 1) zählen zu den Nutzergruppen des IVÖV insbesondere die Einrichtungen der Bundesverwaltung, der Landes- und der Kommunalverwaltungen sowie verwaltungsnahe Organisationen inklusive privatwirtschaftlicher Dienstleister mit besonderen Anfor-

[32] Begriffsbestimmung siehe Glossar Anhang B: Netzdienstleistungen.

[33] Vgl. Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes.

[34] Die IT-Dienstleister haben somit eine Doppelrolle im IVÖV inne – als Anbieter von Fachverfahren und Anwendungen sowie als Nutzer von Netzdienstleistungen (z. B. netznahe Dienste (Protokolle), Konnektivität, Betriebsprozesse).

[35] Eine detailliertere Betrachtung bzgl. der Aufteilung von Verantwortungen und Zuständigkeiten für die Erbringung von Netzdienstleistungen auf Grundlage des ISO OSI-Schichten Modells erfolgt in den Kapiteln 4.3.3 und 4.3.4. Allgemein ist festzuhalten, dass für spezifische Netzdienstleistungen, die technisch über mehrere Netzprotokolle realisiert werden, eine fallabhängige Verantwortlichkeits- und Zuständigkeitsaufteilung in der Netzstrategie nachgelagerten technischen Feinkonzepten erfolgt. Begriffsbestimmung siehe Glossar: Netznahe Dienste.

derungen an die Kommunikation mit der Verwaltung (bzw. mit externen Partnern). Über den IVÖV beziehen die Nutzer IT-Dienstleistungen (i. S. v. Anwendungen und Fachverfahren). Eine weitere Nutzergruppe aus der Perspektive der BDBOS stellen darüber hinaus auch die IT-Dienstleister (BWI, ITZBund und Auslands-IT) als Nutzer von Netzdienstleistungen dar.

4.1.2 Leistungen

Die Leistungen des IVÖV umfassen die Bereitstellung eines Anschlusses an den IVÖV, Netzdienstleistungen[36], insbesondere netznahe Dienste (bspw. TCP/IP) sowie Beratungs- und Zertifizierungskompetenzen als weitere Dienstleistungen. Das Angebot von IT-Diensten (i. S. v. Anwendungen und Fachverfahren) wird durch die jeweiligen IT-Dienstleister gestaltet und ist damit nicht Teil der Betrachtung des Zielbildes 2030.

Den Anschluss an den IVÖV können die Nutzer (i. S. v. Einrichtungen) im Rahmen des Bestellprozesses aus jeweils standardisierten jedoch bedarfsgerechten Produkteigenschaften bspw. in Bezug auf Bandbreite, Schutzniveau, Verfügbarkeit sowie Kommunikationsfähigkeit in Krisensituationen, konfigurieren.

Ein Anschluss an den IVÖV kann bspw. genutzt werden für:

- Gesicherte Verbindungen zur Übermittlung von Daten (z. B. zwischen Rechenzentren und Nutzern eines Fachverfahrens) bei Fachverfahren, welche durch die öffentliche Verwaltung genutzt werden oder im Portalverbund
- Vernetzung zwischen Liegenschaften (Direktverbindung, Bereitstellung Liegenschaften übergreifendes WAN)

Mögliche Netzdienstleistungen sind (Auswahl):

- Managed WAN, d.h. Betrieb und Management eines WAN, bspw. unter Berücksichtigung spezifischer Anforderungen von Ressorts (bspw. für Ressortforschungseinrichtungen) oder im Rahmen der Opt-In Entscheidung von Ländern (bereitgestellt von: BDBOS)
- Gewährleistung der Verfügbarkeit des Basisnetzes im IVÖV sowie verbundener Weitverkehrsnetze (bspw. Landesnetze) in besonderen Lagen (bereitgestellt von: BDBOS)
- Management und Vergabe von IP-Adressen im Rahmen der Aufgabe der operativen LIR de.government (bereitgestellt von: BDBOS)
- Breitbandanschluss für Einrichtungen von Landesverwaltungen ohne bisherige Provider-Versorgung (bereitgestellt von: BDBOS)

Mögliche weitere Dienstleistungen im Kontext Netz- und Sicherheitstechnik sind:

- Security as a Service als Dienstleistung zur Überwachung und Absicherung eines Weitverkehrsnetzes (bereitgestellt von: BSI)
- Beratung zu Informationssicherheit (bereitgestellt von: BSI)
- Prüfung und Zertifizierung von Lösungen und Betreibermodellen i. S. einzelner Zulieferer und des gewählten übergreifenden Betreibermodells für den Netz- und Sicherheitsbetrieb (bereitgestellt von: BSI)
- Vereinfachte Beauftragung von Zulieferern, bspw. Beauftragung über zentrale Rahmenverträge (bereitgestellt von: BDBOS)

Das Angebot von Leistungen des IVÖV ist mit Bezug auf die Nutzergruppe der Bundesverwaltung – soweit sinnvoll und möglich – an die Leistungen der NdB (i. S. eines Produktkatalogs) angelehnt und

[36] Begriffsbestimmung siehe Glossar Anhang B: Netzdienstleistungen.

mit den Leistungen im Kontext der IT-Konsolidierung Bund abgestimmt. Während die Angebote im Bereich Netzdienstleistungen für Bundesressorts, die über Weitverkehrsnetze verfügen bzw. (perspektivisch) Weitverkehrsnetze benötigen, verbindlich sind, werden den Ländern die dargestellten Leistungen optional, über die bloße Teilnahme am Informationsverbund im Sinne eines Anschlusses hinaus, angeboten. Bei der (Weiter-)Entwicklung des Angebots werden die heterogenen Bedarfe der Nutzergruppen von Bund, Ländern und Kommunen berücksichtigt. Besondere Bedarfe zur Kommunikation mit internationalen Partnern ergeben sich bspw. zur Erfüllung der Forschungsaufgaben der Ressortforschungseinrichtungen.[37] Die Leistungen des IVÖV sind in einem Produktkatalog zusammengestellt, welcher zur Abdeckung verschiedenartiger Nutzeranforderungen gestaltet ist. Die Differenzierung des Produktkatalogs für Nutzergruppen wird in Kapitel 4.3.1 erläutert.

4.1.3 Anbieter von Leistungen im IVÖV

Im IVÖV agieren IT-Dienstleister von Bund und Ländern sowie die BDBOS als Anbieter von bestimmten Leistungen. Auf der Ebene des Bundes stellen die IT-Dienstleister des Bundes ITZBund und BWI als Generalunternehmer den Nutzern anwendernahe Dienste und Leistungen (i. S. v. Anwendungen und Fachverfahren) über den IVÖV bereit, die für den Betrieb eines Netzwerks nicht essentiell sind. Unterdessen beziehen die Verwaltungen von Ländern und Kommunen weiterhin selbstständig die IT-Dienste und Leistungen (i. S. v. Anwendungen und Fachverfahren) von ihren jeweiligen IT-Dienstleistern.

Die BDBOS als zentrale Betreiberin des Basisnetzes im IVÖV, die BWI sowie die Auslands-IT des Auswärtigen Amtes erbringen hinsichtlich des Basisnetzes wiederum Netzdienstleistungen - insbesondere netznahe Dienste - gegenüber den IT-Dienstleistern von Bund und Ländern, die für den Betrieb eines Netzwerks zwingend erforderlich sind. Folglich treten die Netzbetreiber im IVÖV gegenüber den IT-Dienstleistern und Nutzern als Netzdienstleister im engeren Sinne auf.[38] Gestaltung und Steuerung für sichere Netzarchitektur und Sicherheitstechnik im Basisnetz, in Netzen von Ländern mit Opt-In Entscheidung bzw. Länder, die die Bundesverwaltung mit dem Management der Informationssicherheit (vgl. Kapitel 4.1.2, Security as a Service) in ihren Netzen beauftragt haben, bringt das BSI in den IVÖV ein.[39]

Abzugrenzen von den Anbietern sind Zulieferer, wie die nachgelagerten Provider von Netzinfrastrukturen sowie Lieferanten und Hersteller von Systemtechnik und Software. Diese sind überwiegend externe Organisationen, die den Netzdienstleistern die Infrastruktur bzw. Produkte im Bereich der Weitverkehrsnetze bereitstellen. Hierbei stellt insbesondere die BWI als Betreiberin des CoreBWI, welches u. a. dem WANBw der Bundeswehr als Backbone-Netz (d. h. als Backbone-Netz Provider) zugrunde liegt, im IVÖV eine Ausnahme dar.

Abbildung 2 zeigt die Verkettung bei der Bereitstellung von Netzdienstleistungen im IVÖV für die Nutzer durch die Anbieter. Als Betreiberin des Basisnetzes im IVÖV und Anbieterin von netznahen Diensten fungiert die BDBOS für Nutzer (i. S. v. Einrichtungen) im Allgemeinen nicht als direkte Ansprechpartnerin.[40] Dagegen gewährleistet die BDBOS gegenüber den IT-Dienstleistern des

[37] Vgl. Der Beauftragte der Bundesregierung für Informationstechnik (2017) und AK ITK der AG Ressortforschung (2017) für weitere Anforderungen der Ressortforschungseinrichtungen.

[38] Die IT-Dienstleister haben somit eine Doppelrolle im IVÖV inne – als Anbieter von Fachverfahren und Anwendungen sowie als Nutzer von Netzdienstleistungen (z. B. netznahe Dienste (Protokolle), Konnektivität, Betriebsprozesse).

[39] Vgl. Bundesministerium des Innern (2016): Cyber-Sicherheitsstrategie für Deutschland; Es ist zu prüfen, ob für die Zusammenarbeit von BSI und den Behörden der Länder weitere rechtliche Rahmenbedingungen zu schaffen sind.

[40] Für die Bearbeitung von Nutzeranfragen (bspw. Bestellung von Netzdienstleistungen) bzw. Problemmeldungen von Nutzern (bspw. technischer Incident) wird nachgelagert zur Strategie ein Servicekonzept von den IT- und Netzdienstleistern erarbeitet und umgesetzt.

Bundes sowie den IT-Dienstleistern der Länder, welche die Opt-In Option wahrnehmen, die erforderliche Konnektivität und Interoperabilität auf Ebene des Netzes (i. S. der Bereitstellung dazu erforderlicher netznaher Dienste). Die in Abbildung 2 dargestellte Verkettung von Leistungen für die Bundesverwaltung ist analog zur Verkettung von Leistungen, die durch NdB ab 2019 vorgesehen wird.

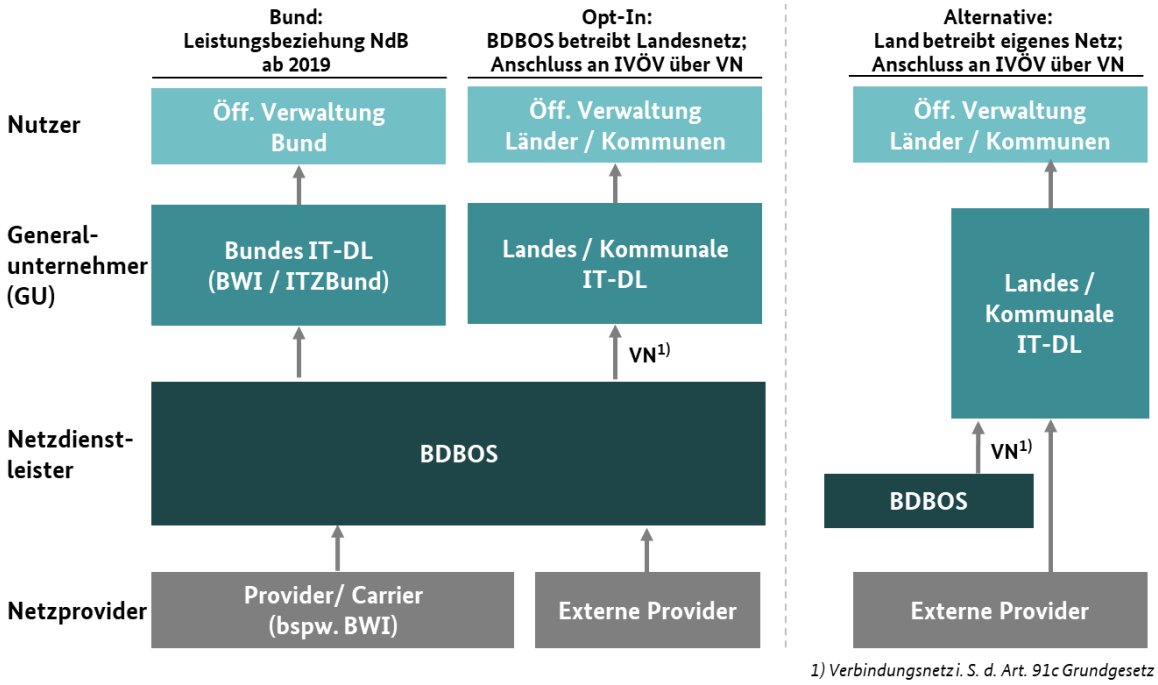


Abbildung 2: Leistungserbringung im IVÖV (vereinfacht)

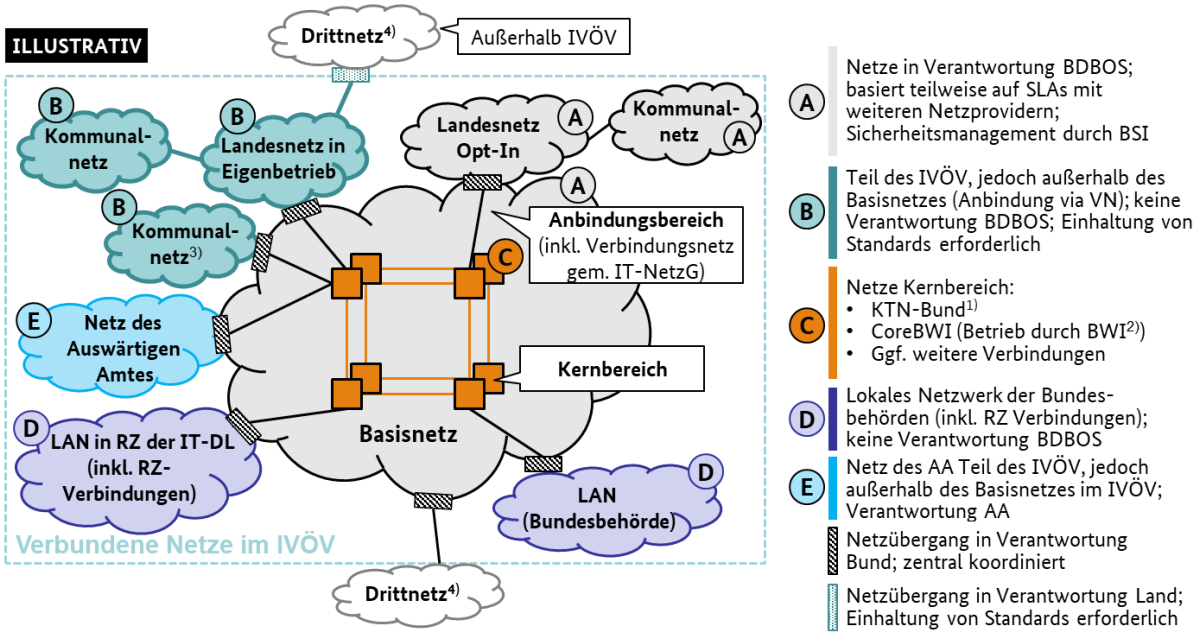
4.2 Technische Architektur

4.2.1 Struktur des Netzverbunds

Die Struktur der verbundenen Netze im IVÖV wird im Folgenden aus einer technischen Betreibersicht auf den IVÖV (Abbildung 3) beschrieben. Zu den Netzen im IVÖV zählen die Verwaltungsnetze des Bundes, das Netz der Auslands-IT des Bundes, ein Verbindungsnetz zur Verbindung der Weitverkehrsnetze des Bundes und der Länder gem. Art. 91 c GG[41] und die verbundenen Netze von Landes- und Kommunalverwaltungen sowie ggf. weitere Spezialnetze der Verwaltung und verwaltungsnaher Einrichtungen. Dabei nehmen das KTN-Bund und die Netze der Auslands-IT eine Sonderrolle unter den Netzen des IVÖV ein. Das KTN-Bund erfüllt als Transportplattform die spezifischen Sicherheits- und betrieblichen Anforderungen des taktisch-operativen Digitalfunks BOS als auch die Anforderungen der ressortübergreifenden Netzinfrastruktur NdB, die auf dem KTN-Bund aufsetzt. Für die digitale Zusammenarbeit auch über die Grenzen des IVÖV hinaus sind die IVÖV-Nutzer über abgesicherte Netzübergänge mit dem Internet bzw. den (Dritt-)Netzen von Wirtschaft, Wissenschaft, Bürgerinnen und Bürgern sowie Partnern im Ausland verbunden. Insbesondere die Netze der Auslands-IT müssen besondere Sicherheitsanforderungen entsprechend ihres internatio-

[41] Verständnis des Verbindungsnetzes hier im Kontext der grundgesetzlichen Regelung nach Art. 91 c Abs. 4 GG, da jeweilige technische Umsetzung bzw. Adaption des Verbindungsnetzes zum jetzigen Zeitpunkt im Kontext des IVÖV nicht antizipiert werden kann.

nalen Einsatzzweckes erfüllen. Die Koppelung der verbundenen Netze im IVÖV untereinander sowie mit Drittnetzen muss derart gestaltet sein, dass eine Gefährdung der anderen Nutzer sowie des Basisnetzes ausgeschlossen werden kann.



1) Vgl. Anhang A.3 des IT-Staatvertrags über die Errichtung des IT-Planungsrats
2) CoreBWI: Kernnetz u.a. für das WANBw; Betreiberin: BWI GmbH (IT-Dienstleisterin des Bundes)
3) Generell befinden Länder in Auslegung des IT-NetzG über Art und Umfang der Beteiligung subsidiärer Kommunen; direkte Anbindung Kommunalnetze möglich, insofern diese nicht über geografisch zugeordnete Ländernetze oder öfftl. bzw. private kommunale Dienstleister angeschlossen werden
4) Fremdnetze, wie bspw. EU-weite bzw. internationale Netze sowie das Internet

Abbildung 3: Betreibersicht - Informationsverbund der öffentlichen Verwaltung

Die verbundenen Netze im IVÖV liegen in unterschiedlichen Verantwortlichkeiten. Innerhalb der Netze sind verschiedene Sicherheitsniveaus (Netzzonen) eingerichtet. Im Zentrum der Netze im IVÖV steht das Basisnetz, das von der BDBOS betrieben wird. Landesnetze, lokale Netzwerke (Englisch: Local Area Network (LAN)) der Bundesbehörden und der IT-Dienstleister, das Netz der Auslands-IT sowie Drittnetze sind über Netzübergänge an das Basisnetz im IVÖV (direkt am Kernbereich oder über den Anbindungsbereich) angeschlossen. Dies betrifft sowohl die in eigener Verantwortung liegenden Ländernetze als auch die Ländernetze bzw. einzelne für die Krisenkommunikation unerlässlichen Standorte in den Ländern (z.B. Lagezentren in den Innenministerien) in Verantwortung der BDBOS (Opt-In Entscheidung).

Basisnetz

Das Basisnetz dient im Zielbild der Netzstrategie zur Kommunikation der gesamten öffentlichen Verwaltung. Es besteht aus dem Kernbereich und dem Anbindungsbereich (i. S. d. Umsetzung des Verbindungsnetzes gemäß Art. 91 c GG), wie in den nachfolgenden Absätzen beschrieben.

Kernbereich

Der Kernbereich des Basisnetzes (Kernbereich) im IVÖV besteht aus einem oder mehreren Netzen mit hohem Vermaschungsgrad und bietet aufgrund der sich dadurch ergebenden Redundanzfähigkeit die höchste Verfügbarkeit im gesamten Netzverbund. Die Nutzung des KTN-Bund als zentrales Netz im Kernbereich leistet einen zentralen Beitrag zur Erreichung der nationalen digitalen Souveränität und Kommunikationsfähigkeit der Verwaltung, auch in besonderen Lagen. Zusätzlich werden Leistungen und Strecken weiterer verwaltungseigener Backbone-Netze, bspw. des Backbone-

Netzes der BWI (CoreBWI), zur Erhöhung der Verfügbarkeit genutzt.[42] Obwohl die BDBOS als zentrale Betreiberin des Kernbereichs des Basisnetzes etabliert ist, verbleibt der Betrieb des CoreBWI langfristig bei der BWI, um den besonderen Anforderungen der Bundeswehr hinsichtlich Geheimhaltung und Handlungsfähigkeit gerecht zu werden.

Zum Kernbereich des Basisnetzes im IVÖV zählen zudem alle Netzdienstleistungen, die zum Betrieb des gesamten Netzverbunds erforderlich sind.

Anbindungsbereich
Der Anbindungsbereich des Basisnetzes im IVÖV umfasst alle Komponenten[43], die für den Zugang zum Kernbereich erforderlich und nicht für die Durchleitung von Datenverkehr innerhalb des Kernbereichs ausgelegt sind. Der Anbindungsbereich endet kernbereichsseitig an den Übergabeschnittstellen zur Anbindung an den Kernbereich und nutzerseitig am Leistungsübergabepunkt für Nutzer. Der Anbindungsbereich des Basisnetzes im IVÖV liegt in Verantwortung der BDBOS sowie dem BSI und besteht aus Netzanschlüssen, die einfach oder redundant (je nach Verfügbarkeitsanspruch) über exklusive Glasfasern an den Kernbereich des Basisnetzes (KTN-Bund oder CoreBWI) angeschlossen sind, und wird als Bestandteil des Basisnetzes betrieben (siehe oben). Der Anbindungsbereich umfasst bspw. die Umsetzung des Verbindungsnetzes nach § 2 Absatz 2 IT-NetzG als direkten Bestandteil des Basisnetzes im IVÖV.

Die Anbindung der Nutzer an das Basisnetz im IVÖV über die „letzte Meile“ wird über einen zentral ausgeschriebenen Multi-Vendor-Ansatz (i. S. v. Carriern, siehe Kapitel 4.3.6) bereitgestellt. Die Auswahl der Carrier erfolgt durch die BDBOS im Einvernehmen mit dem BSI.

Verbundene Netze im IVÖV
Zu den verbundenen Netzen im IVÖV gehören alle Netze, die über gesicherte Netzübergänge mit dem Basisnetz verbunden sind, um darüber Netzdienstleistungen und ggf. weitere (IT-)Dienste der Anbieter von Leistungen im IVÖV (siehe Kapitel 4.1.3) zu nutzen oder in andere verbundene Netze zu kommunizieren. Zu den verbundenen Netzen gehören Weitverkehrsnetze des Bundes (solange sie nicht in das Basisnetz integriert sind, wie bspw. das Netz der Auslands-IT), Landes- und Kommunalnetze sowie lokale Netze der Bundesbehörden und Bundes IT-Dienstleister.

4.2.2 Netzübergänge und Netzkopplungen

Die internen und externen Netzübergänge des IVÖV werden, gemäß den föderalen Zuständigkeiten für die Netze der Bundes- und Landesverwaltungen, jeweils in Verantwortung einer zentralen Stelle (Bund: BSI; Länder: eigenverantwortlich oder wahlweise BSI) überwacht und durch die Verwendung geeigneter Sicherheitstechnologien und -prozesse abgesichert. Eine zentrale koordinierende Stelle auf Ebene des Bundes (voraussichtlich das BSI) wird die Ansätze der jeweils zuständigen Einheiten der föderalen Ebenen politisch-strategisch koordinieren. Die Aufteilung von Verantwortung und Zuständigkeit zwischen dem BSI und der BDBOS im Hinblick auf die Gewährleistung der Sicherheit an Netzübergängen folgt den Festlegungen in einer Verwaltungsvereinbarung zwischen BSI und BDBOS.[44] Darüber hinaus wird sichergestellt, dass Maßnahmen zur Absicherung von Netzübergängen sich im Einklang mit den vielschichtigen Anforderungen an die Funktionalität der Netze und Übergänge, bspw. hinsichtlich ihrer Leistungsfähigkeit, befinden. Darüber hinaus muss bei der Kop-

[42] Eine Festlegung bezüglich Art und Umfang der Nutzung weiterer Backbone-Netze im Kernbereich wird im Rahmen nachgelagerter technischer Konzepte erfolgen.

[43] Hierzu zählen insbesondere die Anbindungsknoten mit allen für eine Anbindung an die Backbone-Netze des Kernbereichs erforderlichen Netzelementen sowie die Übertragungsstrecken und Übertragungsmedien zwischen Anbindungsknoten und Basisnetzknoten.

[44] Vgl. BSI/BDBOS (2018); Beschluss zum Zeitpunkt der Erstellung noch ausstehend.

pelung der verbundenen Netze im IVÖV untereinander sowie mit Drittnetzen eine Gefährdung der anderen Nutzer sowie des Basisnetzes ausgeschlossen werden können.

Interne Netzübergänge
Im IVÖV werden Netze (Basisnetz und verbundene Netze im IVÖV) in der Regel auf OSI-Schicht 3 gekoppelt[45], d.h. eine Kopplung auf den OSI-Schichten 1 und 2 wird zum jetzigen Zeitpunkt nicht ausgeschlossen. Bei der Kopplung von Netzen, insbesondere im Hinblick auf eine bestimmte Kopplungsebene, ist der Einsatz von zukunftsfähigen Technologien (z. B. Software Defined Networking (SDN), Customer Edge Routers in einem Multiprotocol Label Switching (MPLS)-basiertem Layer 3 Netz) einzubeziehen.

Für das Management des Betriebs sowie der Sicherung des Netzwerks sollte ein Network Operations Center (NOC) etabliert werden.[46] Die strategische Verantwortung und operative Zuständigkeit für das NOC liegt entsprechend bei der BDBOS und dem BSI, wobei die Aufgabenverteilung der Verwaltungsvereinbarung zwischen BSI und BDBOS[47] folgt. Das Routing im gesamten IVÖV erfolgt über die Netze hinweg und in den Netzen unter Anwendung von IPv6 gemäß IPv6-Adress- und Routingkonzept für die öffentliche Verwaltung Deutschlands[48]. Eine Local Internet Registry (LIR) übernimmt dabei die lokale Organisation für das Management der Zuteilung und Registrierung von Internet-Ressourcen, u. a. die Verwaltung von IP-Adressen. Während strategische Aufgaben (strategische LIR) durch das BMI-Referat für Netze (aktuell: BMI CI 5) verantwortet werden, übernimmt die BDBOS operative Aufgaben (operative LIR), wie bspw. die Vergabe von Adressbereichen. Länder verwalten als SubLIR den allokierten Adressblock innerhalb ihrer Zuständigkeiten oder gliedern diese an eine operative SubLIR (z. B. IT-Dienstleister) aus.[49]

Auf der logischen Netzebene sind die Nutzer (Einrichtungen bzw. IT-Dienstleister) des IVÖV unterschiedlichen Netzzonen zugeordnet, die sich hinsichtlich Schutzniveau, Service-Level, etc. unterscheiden können. Die Umsetzung dieser unterschiedlichen Netzzonen gewährleistet im IVÖV die Mandantenfähigkeit[50] des Netzes (insb. des Basisnetzes im IVÖV). Für eine zonenübergreifende Kommunikation werden Netzübergänge zwischen dem Basisnetz und den weiteren logischen Zonen innerhalb des IVÖV (bspw. den Netzen der Länder) zentral durch den Bund koordiniert und überwacht. Die Netzübergänge sind unter Berücksichtigung optimierter Laufwege/-zeiten redundant ausgelegt und mit entsprechender Sicherheitsinfrastruktur (bspw. Firewalls) zur Segmentierung unter Berücksichtigung der Zugriffsrichtung umgesetzt.

Insofern die Backbone-Netze des Kernbereichs im IVÖV gekoppelt sind, wird eine intelligente Verkehrssteuerung zur optimierten Auslastung der Backbone-Netze umgesetzt, der eine Fallunterscheidung für den Normalbetrieb und für besondere Situationen (bspw. Ausfall von Teilen einzelner Backbone-Netze) zugrunde liegt. Dafür ist die gegenseitige Bereitstellung einer ausreichenden, reservierten Transportkapazität der redundanten Backbone-Netze erforderlich. Zudem ermöglicht die Nutzung zukunftssicherer Technologien die kurzfristige Umkonfiguration der Netze als Reaktion auf Angriffe oder bei Ausfällen sowie die dynamische Bereitstellung von Bandbreite bei veränderten Anforderungen. Aufgrund der technischen und organisatorischen Komplexität der Kopplung verschiedener (Provider-)Backbone-Netze, bspw. durch die Ausstattung von Organisationen mit besonderen Anforderungen an sichere Kommunikation mit redundanten Anschlüssen im Anbin-

[45] Begriffsbestimmung siehe Glossar Anhang B: Kopplung.

[46] Weitere Detaillierung der Funktionen, Verantwortlichkeiten und Zuständigkeiten in nachgelagerter Feinkonzeption.

[47] BSI/BDBOS (2018); Beschluss zum Zeitpunkt der Erstellung noch ausstehend.

[48] IT-Planungsrat (2016) Beschluss 2016/43 – IP-Adressverwaltung.

[49] Begriffsbestimmung siehe Glossar Anhang B: (Sub)Local Internet Registry; siehe Bundesministerium des Innern (2011) für weitere Details.

[50] Begriffsbestimmung siehe Glossar Anhang B: Mandantenfähigkeit.

dungsbereich, ist die Kopplung der Backbone-Netze des Kernbereichs im Rahmen eines der Netzstrategie nachgelagerten Redundanzkonzeptes zum Kapazitätsmanagement tiefgehend zu betrachten.

Zur Sicherung von Netzübergängen zwischen dem Basisnetz und den verbundenen Netzen im IVÖV sowie Übergängen zwischen logischen Netzen bzw. Netzzonen der öffentlichen Verwaltung sind bestimmte Netzdienstleistungen erforderlich. Diese Dienstleistungen der Netzsicherungsdienste werden sicherheitstechnisch durch das BSI gestaltet und dem Informationsverbund des IVÖV zugeordnet. Identische Rahmenbedingungen für die Netzkonsolidierung (bspw. einheitliche Sicherheitskonzepte und -leitlinien) vermeiden dabei das Auftreten unterschiedlicher und unkoordinierter Sicherheitsstandards. Spezifische Sicherungsmechanismen, bspw. für Netze mit höheren Schutzbedarfen (u. a. Schutzniveau der Regierungskommunikation i. S. v. vertrauliche Übermittlung von Informationen für die unmittelbare Regierungsarbeit), gestaltet das BSI bedarfsgerecht für einzelne Nutzer (i. S. v. Einrichtungen) und Netze (z. B. NdB). Die Tätigkeiten des BSI umfassen dabei insbesondere das Formulieren von Anforderungen, das Herbeiführen von Vereinbarungen zwischen Akteuren im IVÖV, die Bewertung von (Rest-)Risiken sowie die Freigabe bzw. Prüfung von technischen Komponenten.

Im Basisnetz werden Sicherheitsvorgaben des BSI durch ein Security Operations Center (SOC) zentral umgesetzt und überwacht. Das zentrale SOC steuert dazu die jeweils notwendige Sicherheitsinfrastruktur. Die strategische Verantwortung und operative Zuständigkeit liegt entsprechend bei der BDBOS und dem BSI, wobei die Aufgabenverteilung der Verwaltungsvereinbarung zwischen BSI und BDBOS[51] folgt. Dies gilt analog für Ländernetze, die durch die BDBOS betrieben werden, sowie für Länder, die die Bundesverwaltung mit dem Management der Informationssicherheit (vgl. Kapitel 4.1.2, Security as a Service) in ihren Netzen beauftragen. Alternativ geschieht die Überwachung in Verantwortung der Länder.

Externe Netzübergänge

Externe Netzübergänge zu Drittnetzen werden zentral und in sehr begrenzter Anzahl (bspw. je Bundesland zzgl. Bund)[52], unter Gewährleistung des zentralen Absicherungsniveaus gemäß UP Bund[53] geographisch redundant (unter Berücksichtigung optimierter Laufwege/ -zeiten der Daten) etabliert. Dezentrale Netzübergänge zwischen den Netzen im IVÖV und Drittnetzen ermöglichen eine höhere Leistungsfähigkeit des Backbone-Netzes, da der Datenverkehr im Sinne einer besseren Lastverteilung auf mehrere Netzübergänge verteilt wird. Somit wird erreicht, dass zum einen ein einzelner, zentraler Netzübergang nicht zum Engpass bei der Verarbeitung der Datenströme zu Drittnetzen wird. Zum anderen wird eine Entlastung des Backbone-Netzes erreicht, da keine langen Transportstrecken für Datenströme von/zu Drittnetzen über das Backbone-Netz anfallen. Für das Basisnetz, Netze von Ländern mit Opt-In Entscheidung bzw. von Ländern, die die Bundesverwaltung mit dem Informationssicherheitsmanagement beauftragen, werden Netzübergänge zu Drittnetzen durch das BSI gesteuert und überwacht (siehe Kapitel 4.4.4 bzgl. Betrieb eines Security Operation Centers).[54] Sicherheitsmaßnahmen an den Netzübergängen zwischen den eigenständig durch die Länder betriebenen Netzen und daran angeschlossene Drittnetzen werden durch die Verantwortlichen auf Ebene des Landes (bspw. Landes IT-Dienstleister) unter Einhaltung der Mindeststandards

[51] BSI/BDBOS (2018); Beschluss zum Zeitpunkt der Erstellung noch ausstehend.

[52] Die Einrichtung von Netzübergängen erfolgt grundsätzlich bedarfsgerecht; Möglichkeiten zur Vereinheitlichung, Zentralisierung oder Reduktion der Anzahl von Netzübergängen werden fortlaufend identifiziert und geprüft; eine Priorisierung bei der Nutzung von Netzübergängen ist nicht geplant.

[53] Bundesministerium des Innern (2017).

[54] Zur Steuerung und Koordination der Netzübergänge übernimmt das BSI Tätigkeiten im Sinne des § 5 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz).

des BSI hinsichtlich der Schnittstellen zur Kommunikationstechnik des Bundes gewährleistet, so dass eine Gefährdung der weiteren IVÖV-Nutzer möglichst ausgeschlossen wird.

4.3 Betriebsmodell

4.3.1 Differenzierung des Produktkatalogs für Nutzergruppen

Ein einheitlicher Produktkatalog beschreibt die im IVÖV bereitgestellten Leistungen; darüber hinaus ergänzen weitere, nutzergruppenspezifische Angebote das Leistungsspektrum des IVÖV. Hierbei wird unter dem Aspekt der Wirtschaftlichkeit eine bedarfsgerechte Bereitstellung möglichst einheitlicher Leistungen angestrebt. Die für die Nutzer (i. S. v. Einrichtungen) auf Ebene Bund relevanten Produkte werden in den Produktkatalog des Verbundes der IT-Dienstleister (VITD)[55] integriert. Die Kombination aus einem allgemeinen Produktkatalog sowie zusätzlichen nutzergruppenspezifischen Angeboten reduziert die Komplexität bzw. die Aufwände zum Management des Produktkatalogs. Die Festlegung der von der zentralen Netzbetreiberin des Basisnetzes BDBOS beziehbaren Netzdienstleistungen geschieht u. a. anhand der im Weiteren dargestellten Serviceklassen und Servicedimensionen.

4.3.2 Ausprägungen von Serviceklassen und Servicedimensionen

Das Angebot von Netzdienstleistungen, insbesondere netznahe Dienste, wird anhand von Serviceklassen differenziert. Die Differenzierung der Serviceklassen erfolgt in mehreren Servicedimensionen.

Es existieren folgende Servicedimensionen, die teilweise festgelegt oder auch unabhängig voneinander konfigurierbar sind:[56]

- Bandbreite (Geschwindigkeit)
- Verfügbarkeit
- Vertraulichkeit (offen bis VS-Geheim)
- Integrität
- Technische Leistungsparameter (bspw. Jitter, Latenz)

Weitere Servicedimensionen werden im Rahmen der Erarbeitung eines Produktkataloges detailliert. Die Kombination aus festgelegten und unabhängig voneinander konfigurierbaren Servicedimensionen erhöht die Standardisierung und Skalierbarkeit bei vergleichsweise hoher Abdeckung heterogener Anforderungen.

4.3.3 Bereitstellung von Netzdienstleistungen

Für die Leistungserbringung im IVÖV (u. a. Betrieb der Weitverkehrsnetze, Bereitstellung von Netzdienstleistungen) werden den verschiedenen Akteuren (z. B. IT-Dienstleister, BDBOS, BSI) funktio-

[55] Die Etablierung eines Verbundes der IT-Dienstleister (VITD) auf Ebene Bund wird durch das Projekt IT-Konsolidierung Bund bedingt. Auf der Basis des Kabinettsbeschlusses vom 20. Mai 2015 zur „IT-Konsolidierung Bund“ bilden ITZBund, der IT-Dienstleister des BMVg (BWI), die Auslands-IT des AA und die IT von BA und Deutsche Rentenversicherung Bund (DRV Bund) - mit deren gesetzlich zugelassenem Angebot für die Bundesverwaltung - zusammen einen Leistungsverbund, der sukzessive den gesamten Betrieb und die Entwicklung von Basis-, Querschnitts- und Infrastrukturdiensten übernimmt.

[56] Die Aufzählung der Servicedimensionen befindet sich parallel in Abstimmung mit dem Anbieterbeirat.

nale und sicherheitsrelevante Verantwortlichkeiten (i. S. d. Erfolgsverantwortung) zugewiesen. Diese sind durch Leistungsvereinbarungen zwischen den Akteuren geregelt. Zur Strukturierung der Verantwortlichkeiten wird das OSI-Schichtenmodell verwendet. Eine detaillierte Aufschlüsselung der Aufgabenverteilung im Sinne der Zuständigkeit für die operative Umsetzung (d. h. tatsächliche Aktivitäten) erfolgt separat in Kapitel 4.3.4.

Die Verantwortung zur Bereitstellung des Netzzugriffes von Anwendungen und Fachverfahren sowie von spezifischen Netzdienstleistungen zur Erfüllung des Verwaltungsauftrags liegt bei den IT-Dienstleistern von Bund und Ländern (OSI-Schicht 4-7). Die BDBOS verantwortet in ihrer Rolle als Betreiberin des Basisnetzes im IVÖV die Verfügbarkeit und adäquate Erbringung von Netzdienstleistungen,[57] insbesondere netznahe Dienste, für die Anbindung von Bundesministerien, Bundesbehörden und verwaltungsnahen Organisationen auf der Ebene Bund sowie im Rahmen ihrer Funktion als operative LIR de.government das Routing von IP-Paketen (inkl. IPv6 Adressvergabe). Analoges gilt für Landesnetze, sofern die BDBOS mit dem Betrieb eines Landesnetzes beauftragt ist. Darüber hinaus trägt die BDBOS als zentrale Netzbetreiberin des Basisnetzes im IVÖV (und etwaiger Ländernetze) die Verantwortung zur vertraglichen Steuerung für die weiteren zugrundeliegenden OSI-Schichten. Mit Blick auf eigenständig betriebene Netze von Ländern (und Kommunen) verbleibt die Verantwortung für den Betrieb bzw. Bezug dieser Art von Leistungen bei den jeweiligen IT-Dienstleistern bzw. Netzdienstleistern des Landes. Das BSI ist über alle OSI-Schichten hinweg für die Steuerung und Gestaltung sicherheitsrelevanter Aspekte des Informationsverbundes verantwortlich.

Eine Übersicht der Verantwortlichkeiten im Ist-Zustand und im Soll-Zustand (Zielbild 2030) ist in Abbildung 4 dargestellt.

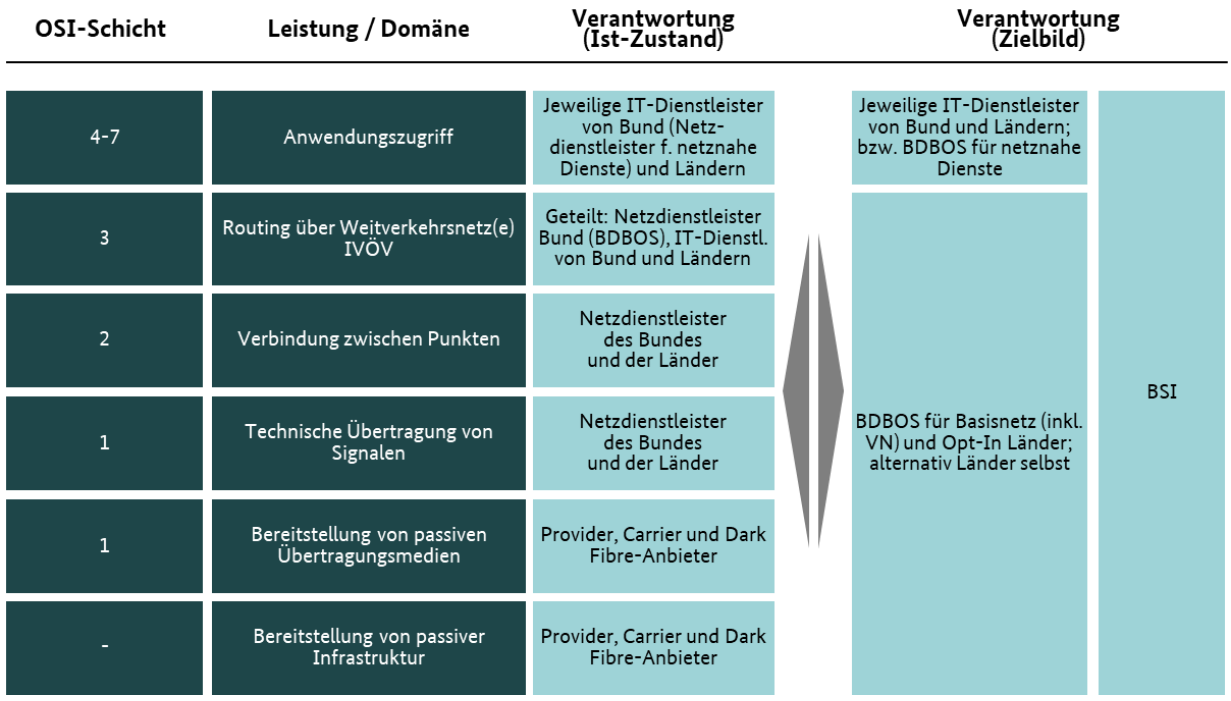


Abbildung 4: Zuordnung Verantwortlichkeit für Netzdienstleistungen im IVÖV

[57] Es ist festzuhalten, dass für spezifische Netzdienstleistungen, die technisch über mehrere Netzprotokolle realisiert werden, eine fallabhängige Verantwortlichkeits- und Zuständigkeitsaufteilung in der Netzstrategie nachgelagerten technischen Feinkonzepten, erfolgt.

Vor dem Hintergrund der weitreichenden Verantwortung der BDBOS für die Netze der öffentlichen Verwaltung bündelt die BDBOS Fähigkeiten für die Bereitstellung von Weitverkehrsnetzen funktional innerhalb der regulären Linienorganisation. Diese organisationsübergreifende, nicht notwendigerweise organisatorisch eigenständige Einheit zur Bündelung funktionaler Kompetenzen arbeitet intensiv mit der Organisationseinheit für sichere Netze des BSI zusammen. Zu diesem Zweck wird eine gemeinsame Test- und Integrationsplattform verwaltet. Die organisationsübergreifende Arbeitsgruppe für Netzkompetenz bündelt gegenwärtig auf verschiedene Organisationen (bspw. ITZBund, BVA, BMI) verteiltes Fachwissen, Systeme und Personalressourcen zum Management und Betrieb der Weitverkehrsnetze der Bundesverwaltung.

4.3.4 Fertigungstiefe der BDBOS

Gegenwärtig beauftragt der Bund – in unterschiedlichem Umfang – größtenteils kommerzielle Netzdienstleister bzw. –provider mit der Bereitstellung von Leistungen für die Netze der Bundesverwaltung. Perspektivisch sollen – dem Leitbild der Gesamtstrategie IT-Netze der öffentlichen Verwaltung[58] folgend – die Netzinfrastrukturen der Bundesverwaltung als kritische IT-Infrastrukturen soweit wie möglich durch den Bund selbst geplant, aufgebaut und betrieben werden. Dazu geht im ersten Schritt zum 1. Januar 2019 die Betriebsverantwortung für NdB auf die BDBOS als staatliche Netzdienstleisterin über. In der weiteren Entwicklung sind die kritischen Aufgaben für Planung, Aufbau und Betrieb des IVÖV durch die BDBOS selbst zu übernehmen. Zur Auswahl dieser Aufgaben wird die Ziel-Fertigungstiefe festgelegt und eine Abgrenzung zwischen Eigenleistungen der BDBOS und Leistungen der IT-Dienstleister des Bundes sowie der durch die BDBOS beauftragten Provider vorgenommen. Zur Strukturierung der Fertigungstiefe bei der Erbringung von Netzdienstleistungen wird das OSI-Schichtenmodell verwendet, wobei die Domäne der passiven Infrastruktur ergänzt und die OSI-Schichten 4 – 7 zur Domäne Anwendungszugriffe zusammengefasst wurden.

Gesamthaft deckt die BDBOS als Netzdienstleisterin des Basisnetzes im IVÖV in der Phase Planung und Betrieb den Großteil der Aufgaben bezogen auf die OSI-Schichten 2 und 3 ab, vereinzelt auch auf OSI-Schicht 1. In der Phase Aufbau liegt der Fokus der BDBOS auf der Spezifikation der Dienste und Technologien auf OSI-Schicht 2 und 3 sowie der Abnahme (bezogen auf alle OSI-Schichten), während insbesondere externe Dienstleister (inkl. Lieferanten) und Provider die Aufgaben der Umsetzung übernehmen.

Zur detaillierten Beschreibung der Aufgabenverteilung im Sinne der Zuständigkeit für die operative Umsetzung (d. h. tatsächliche Aktivitäten) zwischen den IT-Dienstleistern, der BDBOS, dem BSI sowie den externen Providern in den Phasen Planung, Aufbau und Betrieb sind je Phase verschiedene Funktionen[59] festgelegt, anhand derer die Zuständigkeiten entlang der OSI-Schichten definiert werden.[60]

[58] vgl. Bericht zur Gesamtstrategie der Netze der öffentlichen Verwaltung (2013).

[59] Eine Erläuterung der Funktionen ist in Anhang A zu finden.

[60] Die hier festgelegte Verantwortung in Bezug auf die Funktionen stellt den gegenwärtigen Planungsstand (per August 2018) als Arbeitshypothese dar. Ggf. ergeben sich aus Abstimmungen zwischen den IT-Dienstleistern und der BDBOS eine leicht abweichende Aufteilung, die entsprechend in die Netzstrategie übernommen wird.

Planung

Der Phase Planung sind fünf Funktionen zugeordnet: Das auftragnehmerseitige Anforderungsmanagement, das Sicherheitsmanagement, das Zulieferer- und Beauftragungsmanagement, die Planung der Architektur und Netztopologie sowie das Dienste- und Technologiemanagement.

Die **IT-Dienstleister** führen das Anforderungs-, das betriebliche Sicherheits-, das Zulieferer- und Beauftragungsmanagement sowie das Dienstemanagement für Netzdienstleistungen auf den OSI-Schichten 4 bis 7 durch.[61]

Die **BDBOS** übernimmt in der Planungsphase Aufgaben in den Domänen Routing und Switching (OSI-Schichten 2 und 3), in Teilen auch auf OSI-Schicht 1. Demnach führt die BDBOS das Anforderungs- und Sicherheitsmanagement sowie das Dienste- und Technologiemanagement bezüglich der OSI-Schichten 2 und 3 durch. Gleichzeitig übernimmt die BDBOS das Zulieferer- und Beauftragungsmanagement sowie die Planung der Architektur und Netztopologie für die OSI-Schichten 1 bis 3.

Das **BSI** ist im Rahmen der Rechte und Pflichten des BSI-Gesetzes (vor allem § 5 BSI-Gesetz) und UP Bund sowie der Leitlinie Informationssicherheit für die Sicherheit auf allen OSI-Schichten bei den Aufgaben des Sicherheitsmanagements federführend.[62]

Externe Dienstleister und Provider sind in der Phase der Planung mit Aufgaben bezüglich der OSI-Schicht 1 und der passiven Infrastruktur betraut. Das Anforderungsmanagement und Sicherheitsmanagement (unter Steuerung durch das BSI) setzen diese dabei für OSI-Schicht 1 und die passive Infrastruktur um, während sie das Zulieferer- und Beauftragungsmanagement sowie die Planung der Architektur und Netztopologie lediglich für die passive Infrastruktur umsetzen. Darüber hinaus führen externe Dienstleister das Technologiemanagement für OSI-Schicht 1 durch.

Aufbau

Der Phase Aufbau sind vier Funktionen zugeteilt. Es handelt sich um das Dienste- und Technologiedesign (Spezifikation), die Umsetzung (inkl. Entwicklung von IT-Anwendungen), das Rollout und die Abnahme.

Die **IT-Dienstleister** führen in der Phase Aufbau die genannten Funktionen mit Bezug auf IT-Dienste (i. S. v. Anwendungen und Fachverfahren) aus (OSI-Schicht 4 bis 7).

Die **BDBOS** spezifiziert Dienste und Technologien auf den OSI-Schichten 2 und 3 und führt die Abnahme von Produkten und Leistungen hinsichtlich passiver Infrastruktur bis OSI-Schicht 3 durch.

Das **BSI** ist über alle OSI-Schichten an der Abnahme von Produkten und Leistungen beteiligt.

Die **externen Dienstleister und Provider** spezifizieren die von ihnen bereitgestellten Produkte und Leistungen auf OSI-Schicht 1 und im Bereich passiver Infrastruktur. Zudem führen externe Dienstleister und Provider die Umsetzung und den Rollout der Produkte und Leistungen durch.

---

[61] Davon unabhängig sind die durch die IT-Dienstleister eigenverantwortlich betriebenen Netze, z. B. die LAN und RZ-Netze.

[62] Möglicherweise sind für die Befähigung des BSI zur Leistungserbringung im IVÖV organisatorische und rechtliche Rahmenbedingungen anzupassen bzw. zu entwickeln.

Betrieb

Der Phase Betrieb sind sechs Funktionen zugeordnet: Die Dienstebereitstellung, das Netzwerk- und Dienstemonitoring mit Qualitätsmanagement/-sicherung, der Betrieb des Security Operation Center (SOC), die vorbeugende Instandhaltung und Reparatur, das Change-/Lifecyclemanagement und der Support.

Die **IT-Dienstleister** stellen den Nutzern (i. S. v. Einrichtungen) bestimmte Netzdienstleistungen für IT-Anwendungen und Fachverfahren in der Domäne Anwendungszugriffe (OSI-Schichten 4 bis 7) bereit. Sie setzen das Netzwerk- und Dienstemonitoring und Qualitätsmanagement sowie das Change- / Lifecyclemanagement für die OSI-Schichten 4 bis 7 um. Darüber hinaus übernehmen sie den 1st Level Support bei Nutzeranfragen.[63]

Die **BDBOS** übernimmt in der Betriebsphase die Aufgaben in den Domänen Routing und Switching (OSI-Schichten 2 und 3), partiell auch auf OSI-Schicht 1. Die BDBOS führt die Bereitstellung von Diensten, die vorbeugende Instandhaltung und Reparatur, das Change-/Lifecyclemanagement sowie den 2nd Level Support bezüglich der OSI-Schichten 2 und 3 durch.[64] Die BDBOS übernimmt das Netzwerk- und Dienstemonitoring sowie das Qualitätsmanagement für die OSI-Schichten 1 bis 3.

Das **BSI** betreibt unter Zuarbeit aller weiteren Akteure und im Rahmen der Vorgaben des BSI-Gesetzes ein Security Operations Center (alle OSI-Schichten) für das Basisnetz des IVÖV und verbundene Netze von Ländern mit Opt-In-Entscheidung bzw. von Ländern, die die Bundesverwaltung mit dem Management der Informationssicherheit (vgl. Kapitel 4.1.2, Security as a Service) beauftragt haben.

Externe Dienstleister und Provider werden in der Phase des Betriebs insbesondere mit Aufgaben bezüglich der OSI-Schicht 1 und der passiven Infrastruktur beauftragt. Die Bereitstellung von Diensten, die vorbeugende Instandhaltung und Reparatur und das Change-/Lifecyclemanagement führen sie dabei für OSI-Schicht 1 und für die passive Infrastruktur durch, während sie Netzwerk- und Dienstemonitoring sowie Qualitätsmanagement lediglich für die passive Infrastruktur durchführen. Darüber hinaus erbringen externe Dienstleister den Field Service für die passive Infrastruktur sowie für OSI-Schicht 1 und in Zusammenarbeit mit der BDBOS bezüglich OSI-Schicht 2.

Zur kontinuierlichen Prüfung der Einhaltung und Verbesserung von Technologien und Prozessen werden im Rahmen des Qualitätsmanagements und zur Qualitätssicherung seitens der IT-Dienstleister, BDBOS sowie externen Dienstleister und Provider regelmäßige Tests (bspw. Revisionen, Penetrationstests, Audits) durch eigene Prüfteams durchgeführt. Diese berichten an das BSI. Zudem werden unabhängige Prüfungen seitens des BSI übergreifend durchgeführt.

Übergreifende Funktionen

Die phasenübergreifenden Aufgaben des Zulieferer- und Beauftragungsmanagements und der Systemintegration und des Systemmanagements sind der **BDBOS** zugeordnet. Zudem koordiniert das **BSI** in Abstimmung mit den jeweils zuständigen Beteiligten das phasenübergreifende strategische Sicherheitsmanagement. Eine Übersicht der beschriebenen Aufgabenverteilung, aufgeschlüsselt nach den Funktionen der Planung, des Aufbaus und des Betriebs, findet sich in Abbildung 5.

---

[63] Für die Bearbeitung von Nutzeranfragen (bspw. Bestellung von Netzdienstleistungen) bzw. Problemmeldungen von Nutzern (bspw. technischer Incident) wird nachgelagert zur Strategie ein Servicekonzept von den IT- und Netzdienstleistern erarbeitet.

[64] Siehe Fußnote 55.

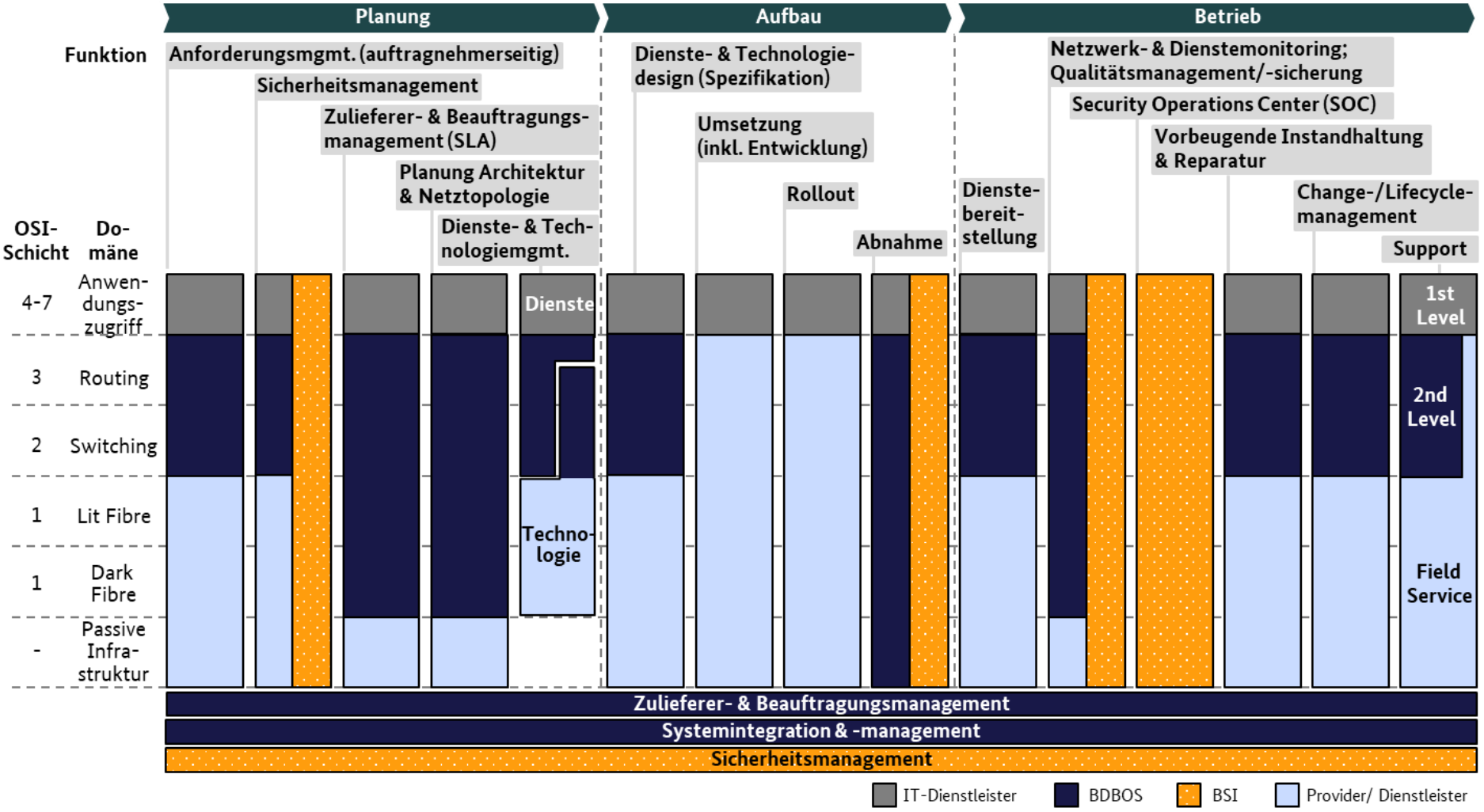


Abbildung 5: Ziel-Fertigungstiefe BDBOS und Aufgabenverteilung im Bereich Netze

Lesehinweis zu Abbildung 5: Die dargestellten Funktionen sind für die Erbringung von Netzdienstleistungen[65] erforderlich. Ein zeitlicher Rahmen für das Durchlaufen der Phasen ist nachgelagert fallbasiert zu bestimmen. Netzdienstleistungen lassen sich grob den aufeinander aufbauenden OSI-Schichten zuordnen.[66] In Analogie ist auch innerhalb der jeweiligen Funktionen eine Aufgabenverteilung mit Blick auf die Leistungserbringung auf der jeweiligen OSI-Schicht möglich. So übernehmen bspw. die IT-Dienstleister gegenüber den Nutzern das auftragnehmerseitige Anforderungsmanagement mit Blick auf die anwendungsbezogenen OSI-Schichten 4 bis 7 sowie teilweise auf OSI-Schicht 3. Die BDBOS wiederum hat die Aufgabe, ein Anforderungsmanagement gegenüber den IT-Dienstleistern zur Verarbeitung deren Anforderungen für die bereitgestellten Netzdienstleistungen auf OSI-Schicht 2 und 3 durchzuführen. Etwaige von der BDBOS beauftragte Provider von Dark Fibre und passiver Infrastruktur führen ihrerseits ein Anforderungsmanagement mit Bezug auf die von der BDBOS formulierten Anforderungen aus.

Die beschriebene Ziel-Fertigungstiefe bildet die Grundlage für eine Einschätzung darüber, in welchen Funktionen der Bund bzw. die BDBOS Fähigkeiten aufbauen wird, welche Ressourcen (Personal, Haushaltsmittel, etc.) hierfür erforderlich sein werden und an welchen Stellen die Zusammenarbeit mit Dienstleistern und externen Providern vorgesehen bzw. unvermeidbar ist (bspw. Field Service). Zur Erreichung der Ziel-Fertigungstiefe können auch Änderungen der gesetzlichen Rahmenbedingungen in Erwägung gezogen werden, wie bspw. die Adjustierung und Erweiterung der Bundeslaufbahnverordnung (BLV) zur Erhöhung der Attraktivität des Bundes als Arbeitgeber zur Begegnung des Fachkräftemangels.

4.3.5 IT-Service-Management

Die Bereitstellung und Weiterentwicklung der Leistungen der Netzdienstleister im IVÖV (i. S. v. netznahen bzw. anwendernahen Diensten und somit IT-Serivces) im Rahmen des IT-Service-Managements ist an den Prozessen, Funktionen und Rollen des ITIL-Rahmenwerks[67] ausgerichtet. Das IT-Service-Management zielt darauf ab, die IT-Services an den Bedarfen der Geschäftsprozesse auszurichten. Gemäß ITIL sind diese nach fünf Phasen des Service-Lebenszyklus strukturiert: Service-Strategy, Service-Design, Service-Operation, Service-Transition und Continual Service Improvement. Ein detailliertes Konzept für das IT-Service-Management ist nachgelagert zur Netzstrategie durch die BDBOS in Zusammenarbeit mit den IT-Dienstleistern zu erarbeiten.

4.3.6 Multi-Vendor-Ansatz

Für den Aufbau und Betrieb der Netze des IVÖV wird ein Multi-Vendor-Ansatz genutzt. Der Multi-Vendor-Ansatz ist die komplementäre Beauftragung verschiedener Zulieferer (z. B. mehrerer Provider, Lieferanten und Hersteller) zur Reduktion der Abhängigkeit von einzelnen Unternehmen, Erhöhung der Flexibilität sowie Verringerung von Risiken. Der Ansatz umfasst neben Beauftragungen und Beschaffungen im Bereich Netzdienstleistungen und Infrastrukturen auch Software und Systemtechnik bspw. für die Einrichtung eines zentralen Security Operations Center (siehe Kapitel 4.4.4). Der Multi-Vendor-Ansatz ermöglicht dabei folglich auch die Beauftragung von spezialisierten Unternehmen. Gleichzeitig ist jedoch ein praktikables Konzept zur Auswahl und Koordination der beauftragten Anbieter nicht zuletzt im Hinblick auf Sicherheitsaspekte erfolgsentscheidend. Die Umsetzung eines Multi-Vendor Ansatzes erfolgt im IVÖV fallabhängig, unter Abwägung der jeweili-

[65] Begriffsbestimmung siehe Glossar Anhang B: Netzdienstleistungen.

[66] Die Funktionen sind in Anhang A erläutert.

[67] ITIL (*Information Technology Infrastructure Library*) ist eine detaillierte Sammlung vordefinierter Prozesse, Funktionen und Rollen für IT-Service-Management, welche unabhängig von Organisation und Technologie einsetzbar sind.

gen Vor- und Nachteile in Bezug auf die betrachteten Leistungen, Sicherheitsanforderungen und die Wirtschaftlichkeit.

Einbezug nachgelagerter Zulieferer (ohne mobile Zugänge)
Die BDBOS bezieht die für die Leistungserbringung erforderlichen Netzdienstleistungen und Infrastrukturen (bspw. Glasfaserleitungen) von verschiedenen nachgelagerten Zulieferern. Dabei werden Leistungen teilweise von weiteren Netzdienstleistern des Bundes, bspw. von der Auslands-IT des Auswärtigen Amtes sowie der BWI, aber auch von externen Providern bezogen.

Bereitstellung mobiler Zugänge zum IVÖV
Mobile Zugänge zum Basisnetz im Anbindungsbereich werden über Mobilfunknetze, Satellitenverbindungen und DSL-Leitungen durch verschiedene externe Provider bereitgestellt. Funkstrecken erlauben die gezielte Anbindung von Liegenschaften an den IVÖV. Der Auswahl der Provider und Technologien für Funkverbindungen geht eine sicherheitstechnische Analyse voraus. Konzepte für mobile Zugänge für bspw. die Realisierung von Telearbeit werden in verteilter Verantwortung für die jeweiligen Nutzergruppen bedarfsgerecht erarbeitet.

Software und Systemtechnik
Für die Einrichtung von Netzübergängen, das Routing und weitere Funktionalitäten werden gemäß Nationalem Anforderungsprofil des BSI überprüfte Software und Systemtechnik verschiedener Zulieferer (Hersteller) beschafft, die den Anforderungen hinsichtlich Sicherheit, technischer Leistungsfähigkeit, Administrierbarkeit (inkl. Skalierbarkeit der Lösung) und Wirtschaftlichkeit genügen. Innovation und neue Technologien werden mit Blick auf ihren Nutzen für die Netze des IVÖV bewertet und ggfs. zu deren Weiterentwicklung eingeführt.

4.4 Steuerung

4.4.1 Rahmenwerk

Für den IVÖV sind eine übergreifende Steuerung und eine Netz-Governance eingerichtet. Diese richten sich nach dem Rahmenwerk von COBIT.[68] Der ganzheitliche Ansatz von COBIT stellt sicher, dass bei der übergreifenden Steuerung durch Bund und Länder die festgelegten gemeinsamen Zielsetzungen in Steuerungsvorgaben resultieren. Die Steuerungsvorgaben werden im IVÖV mit Hilfe von Richtlinien, Prinzipien, Gremien und Rollen sowie Entscheidungsprozessen umgesetzt. Auf Ebene der einzelnen Organisationen findet COBIT Anwendung bei der Steuerung der Leistungserbringung gemäß der in Kapitel 4.3.3 definierten Verantwortung bzw. Zielsetzungen.

4.4.2 Richtlinien und Standards

Einhaltung von Richtlinien und Standards im IVÖV
Richtlinien und Standards mit Geltung für den gesamten IVÖV werden über die jeweiligen fachlichen Gremien festgelegt. Auf Ebene des Bundes werden diese insbesondere unter Berücksichtigung des UP Bund[69] sowie der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“[70] vereinbart. Standards mit Gültigkeit für Teilbereiche des IVÖV werden durch die jeweils zuständigen Organisationen von Bund und Ländern beschlossen (siehe Kapitel 4.4.3). Die Durchsetzung der

[68] COBIT (*Control Objectives for Information and Related Technology*) ist ein international anerkannter Ansatz zur IT-Governance und gliedert die Aufgaben der IT in Prozesse und Steuerungsvorgaben. COBIT definiert hierbei nicht vorrangig wie die Anforderungen umzusetzen sind, sondern primär was umzusetzen ist.

[69] Vgl. Bundesministerium des Innern (2017).

[70] Vgl. IT-Planungsrat (2013).

Standards geschieht jeweils eigenständig gemäß den föderalen Zuständigkeiten mit dem Ziel einer Harmonisierung der eingesetzten Systeme und Prozesse sowie Software-/ Hardwarekomponenten im IVÖV.

Den IVÖV betreffende Richtlinien und Standards sind u. a.:

- Produktkatalog NdB bzw. IT-Konsolidierung Bund
- Architekturrichtlinie
- Sicherheitsanforderungen (bspw. Anforderungen an nationales Routing)
- Netz-Governance (COBIT)
- Servicemanagement (ITIL)
- Nationales Anforderungsprofil (entsprechende Prüfung bzw. Freigabe erforderlich für Einsatz von Produkten und Lösungen im IVÖV)
- Regelungen des Datenschutzes
- Regelungen der Informationssicherheit

Prozess für Technologieanalyse
Für die Prüfung des Einsatzes neuer Technologien im Bereich der Netze des IVÖV wird ein Prozess zur Technologieanalyse etabliert. Erfolgsverantwortung und Zuständigkeiten (i. S. v. tatsächlichen Aktivitäten) für diesen Prozess sind analog der Verwaltungsvereinbarung von BSI und BDBOS[71] für den Beschluss und die Festlegung von Richtlinien und Standards festgelegt. Als Teil der Technologieanalyse werden die mit der Einführung neuer Technologien verbundenen Risiken bewertet.

Entwicklung von Standards in internationalen Gremien
Das Bundesministerium des Innern, für Bau und Heimat initiiert und steuert die Mitwirkung bzw. Positionierung der öffentlichen Verwaltung Deutschlands bei internationalen Gremien zur Entwicklung von Standards im Bereich Netze.

4.4.3 Gremien und Rollen

Die Gremien und Rollen zur Steuerung der Netze der öffentlichen Verwaltung im Zielbild 2030 basieren auf gegenwärtig etablierten Strukturen. Der IT-Rat und die KoITB steuern die Aktivitäten auf Ebene des Bundes unter der Leitung des bzw. der Beauftragten der Bundesregierung für Informationstechnik (BfIT).[72] Der IT-Planungsrat mit seinen Untergremien koordiniert die Zusammenarbeit zwischen Bund und Ländern themenspezifisch.[73] In diesem Sinne befasst sich der IT-Planungsrat mit Grundsatzentscheidungen und der Steuerung gemeinsamer Teile des IVÖV im föderalen Kontext.

Die Bundesverwaltung wird in der Verwaltungsebenen übergreifenden Zusammenarbeit durch den bzw. die durch den IT-Rat entsprechend mandatierten BfIT vertreten, während die Länder durch jeweils einen für Informationstechnik zuständigen Vertreter repräsentiert werden. Gremien bzw. nachgeordnete Arbeitsgruppen des IT-Planungsrats bereiten Entscheidungen hinsichtlich fachspezifischer Fragestellungen vor, bspw. das Arbeitsgremium Verbindungsnetz. Abstimmungen zwischen Bund und Ländern berücksichtigen darüber hinaus die Nachfrageseite (Bedarfsträger) und Anbieterseite (Netzdienstleister, IT-Dienstleister). Zur Fortführung der Zusammenarbeit von Bund

[71] BSI/BDBOS (2018); Beschluss zum Zeitpunkt der Erstellung noch ausstehend.

[72] Künftige Konzepte für Gremien der IT des Bundes werden bei der Detaillierung der Governance berücksichtigt.

[73] Vgl. Vertrag zur Ausführung von Artikel 91c GG (Vertrag über die Errichtung des IT-Planungsrats und über die Grundlage der Zusammenarbeit beim Einsatz von Informationstechnik in den Verwaltungen von Bund und Ländern).

und Ländern hinsichtlich des IVÖV sollte der IT-Planungsrat angehalten werden, die Einrichtung eines weiteren ihm nachgelagerten Arbeitsgremiums zu prüfen.[74]

Auf der Ebene des Bundes bestehen dedizierte Gremien für Entscheidungen bezüglich der Konsolidierung und Weiterentwicklung der Weitverkehrsnetze der Bundesverwaltung, bspw. das NdB-Architekturboard[75] oder die Projektgruppe Netze des Bundes (PG NdB). Diese sind in die Entwicklung der IT-Steuerung Bund eingebettet und übernehmen zentrale Rollen bei der Erarbeitung von zukunftsgerichteten Konzepten. Zur effektiven Steuerung der Etablierung und Weiterentwicklung des IVÖV sollen die Aufgaben der heute existierenden Gremien durch mandatierte Arbeitsgruppen auch in Zukunft wahrgenommen werden. Dies sollte u. a. die Herbeiführung von betrieblichen Entscheidungen hinsichtlich der Netzinfrastrukturen der öffentlichen Verwaltung, soweit diese keinen Grundsatzcharakter haben, die Vorbereitung von Entscheidungen des IT-Rates und der KoITB sowie die Nachfragebündelung und Nutzerinteressenvertretung in Abstimmung mit einem Nachfragerbeirat (Prüfung und Konzeptionierung sowie Aufbau nachgelagert zur Netzstrategie) umfassen.[76]

Neben den Nutzern und Anbietern von IT-Diensten im IVÖV bestehen zusätzliche Rollen. Insbesondere verantwortet das BMI die Koordination und strategische Steuerung des IVÖV. Die BDBOS wird die operative Steuerung der Etablierung des IVÖV verantworten und hierfür ein Projektmanagementoffice etablieren, dessen Anschlussfähigkeit an das Grobkonzept zur Betriebsorganisation NdB zu gewährleisten ist.[77] In diesem Rahmen sollten Berichtswege und –pflichten zur strategischen Steuerung des IVÖV durch das federführende BMI und die nachgelagerten Behörden, u. a. an den Haushaltsausschuss, den IT-Rat sowie den IT-Planungsrat, festgelegt werden. Zusätzlich nimmt das BSI für das Basisnetz des IVÖV sowie die Netze der Länder mit Opt-In Entscheidung die Rolle des Informationssicherheitsbeauftragten (IT-SiBe) wahr.[78] Im Hinblick auf das Nutzer- und Anforderungsmanagement im IVÖV ist die Etablierung eines Nachfragerbeirates bei der BDBOS zu prüfen.

4.4.4 Regelung Sicherheitsmanagement

Das Sicherheitsmanagement umfasst die Bereiche Datenschutz sowie Informationssicherheit und wird gemäß föderaler Zuständigkeit verteilt durchgeführt. Auf Ebene Bund sowie für Länder, die das entsprechende Angebot des IVÖV nutzen (Opt-In, bzw. Inanspruchnahme des entsprechenden Angebots), erfolgen Maßnahmen zur Informationssicherheit durch das BSI in Abstimmung mit den Providern, der BDBOS sowie den jeweiligen IT-Dienstleistern. Die Verantwortung und Zuständigkeit liegt entsprechend bei dem BSI sowie der Netzbetreiberin BDBOS, wobei die Aufgabenverteilung der Verwaltungsvereinbarung zwischen BSI und BDBOS[79] folgt.

Die entsprechenden rechtlichen Voraussetzungen für eine Zusammenarbeit von BSI und den Landesverwaltungen sind in der Leitlinie für Informationssicherheit in der öffentlichen Verwaltung[80] geschaffen. Den Bereich Datenschutz verantwortet auf Ebene Bund die bzw. der Beauftragte für den

[74] Grundlage für die weitere Zusammenarbeit von Bund und Ländern bildet die Entscheidung 2018/52 des IT-Planungsrates zu den Eckpunkten einer Netzstrategie 2030. Die Aufgaben und Zuständigkeiten des Fachgremiums zum IVÖV sollten sich an den Regelungen der AG Informationssicherheit bzw. AG IPv6 orientieren.

[75] Beschluss der 29. Sitzung des Haushaltsauschusses am 12. November 2014.

[76] Eine mögliche Verstetigung der PG NdB, die die aufgeführten Aufgaben gegenwärtig wahrnimmt, ggf. mit Anpassung von Zuständigkeit, Namensgebung und organisatorischer Ausprägung, ist im Weiteren durch die KoITB zu bestimmen. Es ist auch zu prüfen, ob eine Konsolidierung des NdB-Architekturboards und der PG NdB sinnvoll ist.

[77] BDBOS (2016).

[78] Die Rolle erstreckt sich nicht auf die IT-Dienstleister und Nutzer (i. S. v. Einrichtungen). Die verschiedenen Rollen und Aufgaben im Bereich Sicherheitsmanagement werden in einer Informationssicherheitsrichtlinie gesondert geregelt.

[79] BSI/BDBOS (2018); Beschluss zum Zeitpunkt der Erstellung noch ausstehend.

[80] IT-Planungsrat (2013), Beschluss 2013/01: Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung.

Datenschutz und die Informationsfreiheit (BfDI) ebenfalls in Abstimmung mit den Netzprovidern, Netzdienstleistern und IT-Dienstleistern.

Das Sicherheitsmanagement deckt die Bereiche Strategie (Planung), operative Steuerung (bspw. Betrieb eines Security Operations Center (SOC)) und betriebliche Umsetzung (bspw. Abnahme von Leistungen im IVÖV, Aufbau eines SOC) ab. Das BSI übernimmt als federführende Einheit sowohl strategische als auch operative Aufgaben im Hinblick auf Fragestellungen zur Informationssicherheit selbst, während Dienstleister mit der betrieblichen Umsetzung beauftragt werden (können). Im Fokus steht dabei die Implementierung von geeigneten Sicherheitskonzepten und Umsetzung von Sicherheitstechnologien im Hinblick auf die Abwehr von Angriffen sowie zur Verhinderung von ungewollten Verlusten von Informationen. Einen zentralen Aspekt des Sicherheitsmanagements stellt insbesondere der Betrieb eines zentralen Security Operations Center und eines schon jetzt bestehenden Computer Emergency Response Team der Bundesverwaltung (CERT-Bund) dar. Ebenso sollen Richtlinien und Standards zu Datenschutz und Informationssicherheit (inkl. Geheimhaltung und Kommunikationsfähigkeit in besonderen Lagen) erarbeitet und durchgesetzt werden.

Der Bund stellt den Netzbetreibern (u. a. den IT-Dienstleistern) der Ländernetze im Rahmen des Produktkatalogs bei Bedarf Fähigkeiten für das Sicherheitsmanagement der Netze bereit.

4.4.5 Regelung Zulieferermanagement

Zur Erbringung der Netzdienstleistungen im IVÖV steuert die BDBOS die nachgelagerten Provider, Lieferanten und Hersteller zentral. Dies umfasst die Auswahl und das Management der Zulieferer. Dabei wird die Zusammenarbeit mit der zentralen IT-Beschaffung des Bundes (ZIB) sichergestellt.

Die Länder bzw. die zuständigen IT-Dienstleister steuern bei Eigenbetrieb der Ländernetze nachgelagerte Zulieferer jeweils selbst unter Berücksichtigung von abgestimmten Mindestanforderungen im Kontext der Informationssicherheit, bspw. bezüglich des Grundsatzes der nationalen Routings.

4.4.6 Finanzierung

Anschluss Basisnetz (Nutzerseite Bund)
Die Finanzierung der ausschließlich durch den Bund genutzten Teile des IVÖV orientiert sich am Nutzungsgrad der angeschlossenen Nutzer (i. S. v. Einrichtungen) hinsichtlich der angebotenen Leistungen. Die Rechnung berücksichtigt, dass Aufwände auf Nutzerseite mit der Anzahl anzubindender Lokationen (und der Bandbreite der Anschlüsse) skalieren. Ggf. geschieht die Abrechnung gegenüber Bundesbehörden in Form einer Pauschale pro nachgelagert verbundenem Arbeitsplatz. Folglich wird - ausgehend von der heutigen Aufteilung in Netzbetreiber- und Nutzerhaushalte - als langfristiges Ziel für die Finanzierung der Anschlüsse eine Kostenrechnung auf Basis einer Nutzerumlage bzw. eine Pauschalberechnung auf Basis des Nutzungsgrades der angeschlossenen Teilnehmer angestrebt. Dabei müssen die Netzbetreiber und Nutzer anfallende Kosten aus ihren Plafonds aufbringen, zusätzliche Mittel sind nicht vorgesehen. Ein entsprechend detailliertes Kosten-, Finanzierungs- sowie Abrechnungskonzept wird in der Strategie nachgelagerten Maßnahmen konkretisiert und mit den Ressorts abgestimmt.

Anschluss Basisnetz inkl. Betrieb Landesnetz bei Opt-In (Nutzerseite Länder / Kommunen)
Die Länder und Kommunen sind entsprechend ihrem Nutzungsanteil und analog zu dem für Bundesnutzer beschriebenen Finanzierungsmodell an den Gesamtkosten zu beteiligen (Verursacherprinzip). Ein Anschluss an das Verbindungsnetz gemäß IT-NetzG ist inkludiert.

Anschluss Verbindungsnetz (Länder mit Netz im Eigenbetrieb)
Das Finanzierungsmodell des Verbindungsnetzes ist durch das IT-NetzG (§ 7 zu Kosten) geregelt.

Netzdienstleistungen und weitere Leistungen
Die Bepreisung von Netzdienstleistungen und weiterer Dienstleistungen im Kontext der Netz- und Sicherheitstechnik im IVÖV (siehe Kapitel 4.1.2) ist als Maßnahme priorisiert zu erarbeiten. Allge-

mein steht die Finanzierung möglicher Mehraufwände für Bund, Länder und Kommunen im Rahmen des IVÖV unter allgemeinem Haushaltsvorbehalt und ist auf ein möglichst einheitliches, verursachergerechtes Finanzierungsmodell abzustellen. Ebenso sind rechtliche Rahmenbedingungen zu berücksichtigen sowie Regelungen für die Zusammenarbeit von Bund und Ländern bei IT-Projekten bei Änderung der angenommenen Grundlagen fortzuschreiben.

5 Ausblick

Zur Etablierung des IVÖV und Erfüllung des beschriebenen Zielbilds 2030 müssen eine Vielzahl an Maßnahmen umgesetzt werden. Mit der Koordination dieser Maßnahmen ist das BMI (Referat BMI CI 5 - Netzinfrastrukturen; Digitalfunk BOS) betraut, wobei die Steuerung durch das BMI in Absprache mit den jeweilig zuständigen Gremien umgesetzt wird. Verantwortliche Vertreter anderer Ressorts und Länder werden fortlaufend eingebunden. Die Erfüllung des Zielbilds ist durch ein Programm zur Umsetzung der Netzstrategie zu gewährleisten. Dabei sind Erfolgskriterien und Umsetzungsrisiken zu beachten. Regelmäßige Fortschrittsberichte sowie ein unabhängiges und neutrales Programm-Controlling sollen die Transparenz über den Umsetzungsstand sicherstellen. Änderungen der übergeordneten Zielsetzungen sind im Rahmen eines Strategieprozesses zu berücksichtigen. Zukünftige Entwicklungen sind zu antizipieren und ihr Einfluss auf die Netzstrategie ist zu prüfen.

Programm zur Umsetzung der Netzstrategie
Maßnahmen zur Erfüllung des Zielbilds sind in einem separaten Umsetzungsdokument zu beschreiben. Unter anderem werden im Zuge dieser Maßnahmen die Festlegungen der Netzstrategie in Grob- und Feinkonzepten weiter detailliert. Die identifizierten Maßnahmen bilden in ihrer Gesamtheit ein Programm, dessen Leitung und Koordination durch das BMI-Referat für Netze (aktuell: BMI CI 5) in Abstimmung mit den betroffenen Bundesressorts verantwortet wird. Die strategische Steuerung des Programms erfolgt analog der Festlegungen in Kapitel 4.4.3 zur Steuerung des IVÖV.

Erfolgskriterien und Umsetzungsrisiken
Für die erfolgreiche Durchführung des Programms existieren Hürden und Risiken, die im Vorhinein zu betrachten und gezielt anzugehen sind. Zu den Risiken der Umsetzung zählen insbesondere die verteilten Zuständigkeiten für die Maßnahmen sowie die existierenden, kritischen Abhängigkeiten vom Fortschritt der Projekte der IT-Konsolidierung Bund und von sich möglicherweise ändernden Rahmenbedingungen. Ansatzpunkte zur fortlaufenden Identifikation, Analyse und Behandlung von Risiken bilden die Festlegungen des Zielbildes hinsichtlich der Gremien und Rollen (Kapitel 4.4.3) sowie eine zentrale Programmsteuerung. Insbesondere sind die im Rahmen der IT-Konsolidierung geplanten und bereits umgesetzten Änderungen an der IT-Landschaft der Bundesverwaltung sowie die Veränderungen im Hinblick auf das Onlinezugangsgesetz Ursachen für die stetig wachsenden Anforderungen an die Netze der öffentlichen Verwaltung. Aus Perspektive des BMI ist es daher notwendig, einen erfolgreichen Fortlauf der IT-Konsolidierung Bund aktiv zu fördern und den daraus resultierenden Abhängigkeiten bei der weiteren Planung und Gestaltung des IVÖV zu begegnen. Vor dem Hintergrund der Vielzahl an Beteiligten des IVÖV ist es essentiell, die erforderlichen Abstimmungen und Beschlüsse zielgerichtet und bedarfsgesteuert herbeizuführen. Bei der Zusammenarbeit muss insbesondere die Separierung von Zuständigkeiten im Föderalismus berücksichtigt bzw. die aktuell geltenden Rahmenbedingungen perspektivisch einvernehmlich modernisiert werden.

Strategieprozess
Zur fortlaufenden Gewährleistung der Aktualität der Netzstrategie hinsichtlich ihrer organisatorischen und technischen Aspekte und zur regelmäßigen Überprüfung der Maßnahmen wird ein Strategieprozess auf Ebene des Bundes (d. h. in der Programmsteuerung und strategischen Aufsicht des BMI) etabliert.[81] Mit dem Strategieprozess wird ebenso die Nutzung und Förderung von Innovationen für Netzinfrastrukturen gewährleistet. Im Rahmen des Programmes zur Umsetzung müssen die organisatorischen und personellen Voraussetzungen für einen effizienten Review der Netzstrategie geschaffen werden. Hierzu zählt ebenso der Anschluss an das IT-Controlling Bund. Der Strategie-

[81] Der Strategieprozess, der die bedarfsgerechte bzw. zyklische Aktualisierung der Netzstrategie 2030 und die Fortschreibung der Maßnahmen gewährleistet, steht nicht in unmittelbarem Zusammenhang mit den Prozessen des IT-Service-Managements nach ITIL.

prozess wird nachgelagert zur Netzstrategie durch das BMI erarbeitet und mit dem IT-Controlling Bund abgestimmt.

Fortschrittsberichte
In Anlehnung an das zum Strategieprozess vorgesehene Berichtswesen und unabhängige Programm-Controlling ist über den Fortschritt des Programmes und die Umsetzung der einzelnen Maßnahmen den relevanten Stellen (insb. IT-Planungsrat, Programmleitung, NdB-Architekturboard, IT-Rat, ggf. HHA) regelmäßig Bericht zu erstatten. Berichtsfrequenz und Umfang der Berichterstattung werden im Rahmen des Umsetzungsprogrammes zur Netzstrategie mit dem Empfängerkreis abgestimmt. Hierbei wird die Anschlussfähigkeit an das Berichtswesen des IT-Controlling Bund berücksichtigt.

Zukünftige Entwicklungen
Das Zielbild 2030 wurde auf Basis der heutigen Informationslage und unter Annahme bestimmter Prämissen entwickelt. Veränderungen dieser Ausgangslage sind möglich und zu antizipieren. Sie sind bei der weiteren Entwicklung zu berücksichtigen.

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
BfDI	Beauftragte/r für den Datenschutz und die Informationsfreiheit
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BGP	Border Gateway Protocol
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern, für Bau und Heimat
BMVg	Bundesministerium der Verteidigung
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BWI	IT-Dienstleister der Bundeswehr
CERT-Bund	Computer Emergency Response Team der Bundesverwaltung
COBIT	Control Objectives for Information and Related Technology
IPv6	Internet Protocol Version 6
GU	Generalunternehmen
IT	Informationstechnik
ITIL	Information Technology Infrastructure Library
IT-NetzG	Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder
IT-SiBe	IT-Sicherheitsbeauftragter
ITZBund	Informationstechnikzentrum Bund
IVBB	Informationsverbund Berlin-Bonn
IVÖV	Informationsverbund der öffentlichen Verwaltung
KoITB	Konferenz der IT-Beauftragten der Ressorts
KTN	Kerntransportnetz
MPLS	Multiprotocol Label Switching
NdB	Netze des Bundes
OSI-Schicht	Architekturschicht des Referenzmodells Open Systems Interconnection Model
PG NdB	Projektgruppe „Netze des Bundes“
SDN	Software Defined Networking
SLA	Service-Level-Agreement
SOC	Security Operation Center
VN	Netze des Bundes - Verbindungsnetz
ZIB	Zentrale IT-Beschaffung des Bundes

Quellenverzeichnis

Abschlussbericht Strategie-Review des Projektes „IT-Konsolidierung Bund“ (Version 0.95 vom 30.11.2017)

AK ITK der AG Ressortforschung (2017): Anforderungen der Ressortforschungseinrichtungen an das Projekt „IT-Konsolidierung Bund“ IT für erfolgreiche Forschungen (Version 1.0 vom 06.11.2017), Anlage 1 zu Bedarfsanalyse zur Betriebs- und Dienstekonsolidierung der Ressortforschungseinrichtungen

Bundesministerium des Innern (2011): Deutschland-Online Infrastruktur - IPv6 Referenzhandbuch

Bundesministerium des Innern (2016): Cyber-Sicherheitsstrategie für Deutschland

Bundesministerium des Innern (2017): Umsetzungsplan Bund 2017

Bundesregierung (2013): Bericht der Bundesregierung zur „Gesamtstrategie IT-Netze der öffentlichen Verwaltung“

Bundesregierung 2014: Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen

BDBOS (2016): Betriebsorganisation NdB ab 2019 / Grobkonzept

BSI/BDBOS (2017): Verwaltungsvereinbarung zwischen der Bundesrepublik Deutschland, vertreten durch das Bundesministerium des Inneren, für Bau und Heimat vertreten durch das Bundesamt für Sicherheit in der Informationstechnik und Verwaltungsvereinbarung zwischen der Bundesrepublik Deutschland, vertreten durch das Bundesministerium des Inneren, für Bau und Heimat vertreten durch das Bundesamt für Sicherheit in der Informationstechnik (Hinweis: Beschluss befindet sich aktuell noch in Abstimmung)

Der Beauftragte der Bundesregierung für Informationstechnik (2018): Eckpunkte einer Netzstrategie 2030 für die öffentliche Verwaltung (Version 1.3 vom 06/2018)

Der Beauftragte der Bundesregierung für Informationstechnik (2017a): Ressortforschungseinrichtungen Bedarfsanalyse zur Betriebs- und Dienstekonsolidierung (Version 4.1 vom 01.12.2017)

IT-Planungsrat (2010), IT-Staatsvertrag zwischen Bund und Ländern zur Ausführung von Artikel 91c GG und zur Errichtung des IT-Planungsrats

IT-Planungsrat (2013), Beschluss 2013/01: Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung

IT-Planungsrat (2016), Beschluss 2016/43: IP-Adressverwaltung

IT-Planungsrat (2018), Entscheidung 2018/52: Weiterentwicklung Netzstrategie 2030 für die öffentliche Verwaltung

Haushaltsausschuss (2014): 29. Sitzung des Haushaltsausschusses am 12. November 2014 - Beschluss des Haushaltsausschusses zu TOP 11a) und b)

Koalitionsvertrag zwischen CDU, CSU und SPD für die 19. Legislaturperiode, 12. März 2018

Konferenz der IT-Beauftragten der Ressorts (2018): Beschluss vom 28.06.2018

Anhang A: Erläuterung Funktionen im Bereich Netzdienstleistungen

Phase	Funktion	Definition
Planung	Anforderungs-management (auf-tragnehmerseitig)	Aufnahme und Koordination der Anforderungen von • Behörden (Nutzern) an IT-Dienste (i. S. v. Anwendungen und Fachverfahren) durch IT-Dienstleister, • IT-Dienstleistern an Netzleistung durch BDBOS, und • der BDBOS an Glasfaserleitungen (Lit Fibre, Dark Fibre) sowie passive Infrastruktur durch Provider Dabei: Priorisierung von Anforderungen und Anstoß von IT-Projekten sowie Kontrollprozesse
	Sicherheitsmanage-ment	Management von Ressourcen für Entwicklung von Standards bzw. Prozessen zur Sicherung der IT und zur Wahrung der Systemintegrität
	Zulieferer- & Beauf-tragungsmanagement (SLA)	Steuerung und Durchführung der Beschaffung, Koordination des Vertragsmanagements, Management und Controlling der Leistungserbringung sowie Management der SLAs und OLAs
	Planung Architektur & Netztopologie	Definition von Netzwerkelementen, Definition von Schnittstellen zu anderen Netzwerken sowie Spezifikation von Netzwerkdiensten
	Dienstemanagement	Management des Produkt- / Servicekatalogs, Anstoß der Dienste- / Serviceentwicklung, Steuerung und Durchführung der kontinuierlichen Produktverbesserung bzw. der langfristigen Einstellung von Produkten
	Technologie-management	Management des Technologieportfolios und der technischen Roadmap (z. B. Erhöhung der Leistungsfähigkeit des Verbindungsnetzes), Auslösen von Technologieentwicklungszyklen, kontinuierlicher Technologieverbesserung sowie Substitution von Technologien
Aufbau	Dienste- & Technologiedesign (Spezifikation)	Detaillierte Spezifikation von Anwendungen und Leistungen sowie von Netzwerken und IT-Plattformen (Hardware)
	Umsetzung (inkl. Entwicklung)	Durchführung der Entwicklung von IT-Anwendungen und Leistungen sowie Konfiguration und Parametrisierung
	Roll-Out	Durchführung von Logistik, Installation, Konfiguration und Testen von Netzwerken, IT-Plattformen und Anwendungen bei der Einführung
	Abnahme	Definition von Testszenarien und -umgebungen, Monitoring der Piloten sowie Validierung und Interpretation der Ergebnisse, der Qualitätstests und des Erstellungsprozesses
Betrieb	Dienstebereitstellung	Management der Konfiguration von Elementen, Auslösen und Management von Anträgen auf Anwendungsänderungen
	Netzwerk- & Dienstemonitoring; Qualitätsmana-gement/-sicherung	Monitoring von Ende-zu-Ende Anwendungsprinzipien für den Betrieb, Monitoring der Netzwerk-Performance sowie Planung und Auslösen von Wartungen der Netzwerkelemente und Netzinfrastruktur; zudem: Qualitätstests, Berichterstattung und Feedback zu Betriebsprozessen im Rahmen Qualitätsmanagement und -sicherung mittels des P(lan)-D(o)-C(heck)-A(ct)-Zyklus
	Security Operations Center (SOC)	Betrieb Security Operations Center für den IVÖV zur Koordination aller Übergänge zwischen Basisnetz und verbundenen Netzen im IVÖV bzw. Drittnetzen und Steuerung notwendiger Sicherheitsinfrastruktur

Phase	Funktion	Definition
	Vorbeugende Instandhaltung & Reparatur	Erkennung und Behebung von Mängeln und Schäden, Kontrolle von Ersatzteilvorrat und -logistik, Verteilung von Ersatzteilen an Feldservice-Kräfte und 2nd Level Support, Durchführung von Reparaturen
	Change-/Lifecycle-management	Management von Problemlösungen und Problembeseitigung für komplexe Fälle, Spezialfälle und strategische Fragestellungen (z.B. grundlegende Veränderungen bei Anforderungen, Technologien, etc.); Weiterentwicklung und Betreuung von Anwendungen über gesamten Lebenszyklus (inkl. Anwenderbetreuung i. S. v. Anforderungsmanagements)
	Support (Anwenderbetreuung)	1st Level Support: Fehlerlokalisierung und Fehlerbehebung bei Standardanfragen; 2nd Level Support: Reaktive Fehlerlokalisierung und Fehlerbehebung, die nicht durch 1st Level Support bearbeitet werden können; proaktive Instandhaltung der Systeme; Field Force: Vor-Ort-Betreuung für 1st Level Support, 2nd Level Support und Instandhaltung (bei Bedarf auch zuständig für Roll-Out von Produkten / Services)
Übergreifende Funktionen	Zulieferer- & Beauftragungsmanagement (SLA)	Steuerung und Durchführung der Beschaffung, Koordination des Vertragsmanagements, Managements und Controlling der Leistungserbringung sowie Management der SLAs und OLAs
	Systemintegration & System-management	"Brückenfunktion" für Problem- und Changemanagement sowie Design von Systemschnittstellen und Funktionsdesign
	Sicherheits-management	Abdeckung der Bereiche Strategie (Planung), operative Steuerung (bspw. Betrieb eines Security Operations Center (SOC)) und betriebliche Umsetzung (bspw. Abnahme von Leistungen im IVÖV, Aufbau eines SOC) des Sicherheitsmanagements

Anhang B: Glossar

Begriff	Definition bzw. Erläuterung
Anbieter	Im IVÖV agieren die IT-Dienstleister von Bund und Ländern sowie die BDBOS als Anbieter von Leistungen. Während die IT-Dienstleister den Nutzern (i. S. v. Einrichtungen) Anwendungen und Fachverfahren sowie die erforderlichen anwendernahen Dienste (Protokolle) bereitstellen, erbringt die BDBOS als Netzbetreiberin netznahe Dienste (u. a. Konnektivität und Interoperabilität), die sowohl von den Nutzern (i. S. v. Behörden) als auch den IT-Dienstleistern genutzt werden. (siehe Begriffsdefinition „Nutzer“)
Anwendernahe Dienste	Dienste, die keine Relevanz für die Aufrechterhaltung des Betriebs des Basis-/Kernnetzes haben. Im Kontext der Netzstrategie können dies z. B. die Dienste oberhalb des OSI-Layer 3 sein.
Backbone-Netz	Backbone-Netze dienen der Verbindung von Knoten bzw. sogenannten Points of Presences (POP) oder Vermittlungsstellen zur Verbindung von zwei oder mehr Kommunikationsnetzen, in der Regel über hochperformante optische Übertragungswege mit Bandbreiten im Bereich mehrerer GBit/s.
Fachverfahren	Ein Fachverfahren ist die Gesamtheit aller organisatorischen Anweisungen und Abläufe (manuell, elektronisch) zu einem bestimmten Zweck nach fachlichen Gesichtspunkten.
Informationsverbund der öffentlichen Verwaltung	Der IVÖV bietet ein Verwaltungsebenen übergreifendes Angebot zur Vernetzung der öffentlichen Verwaltung von Bund, Ländern und Kommunen sowie mit (inter-)nationalen Partnern aus Wirtschaft, Wissenschaft und Verwaltung bzw. Bürgerinnen und Bürgern. Im IVÖV werden grundsätzlich Netzleistungen bereitgestellt. Zusätzlich können über den IVÖV weitere IT-Dienste (i. S. v. Anwendungen und Fachverfahren) angeboten werden. Bestandteile des IVÖV sind die Netzinfrastrukturen der öffentlichen Verwaltung (physikalische Weitverkehrsnetze, Betriebsorganisationen und netznahe Dienste), z. B. das Verbindungsnetz nach § 2 Absatz 2 IT-NetzG und über dieses verbundene Länder- und Bundesnetze.
IT-Dienst	Allgemein wird unter dem Begriff eine technische, autarke Einheit, die zusammenhängende Funktionalitäten zu einem Themenkomplex bündelt und über eine definierte Schnittstelle zur Verfügung stellt verstanden. Ein Dienst abstrahiert dabei die zugrundeliegende technische Funktion soweit, dass ein Verständnis über dahinterstehende Technik nicht notwendig ist. In der Netzstrategie werden Fachverfahren und Anwendungen als IT-Dienste bezeichnet.
IT-Leistung	Eine IT-Leistung besteht aus einer Kombination von Personen, Prozessen und IT-Lösung. Eine IT-Leistung wird zwischen einem Auftragnehmer und einem Auftraggeber durch eine verbindliche Vereinbarung über die Leistungsqualität definiert.
Basisnetz	Das Basisnetz im IVÖV besteht aus den Backbone-Netzen des Kernbereichs sowie dem Anbindungsbereich, der unter anderem die Umsetzung des Verbindungsnetzes (i. S. d. Art. 91 c Abs. 4 Grundgesetz) einbezieht. Es wird von der BDBOS betrieben.
Konsolidierung (Netze)	Unter der Konsolidierung von Netzen wird die technisch-architektonische, betriebliche und vertragliche Zusammenfassung von Netzen im Sinne einer Vereinheitlichung der verantwortlichen Betriebsorganisation verstanden. Die Konsolidierung schließt alle Umstellungsprozesse (technisch, organisatorisch, vertraglich, etc.) ein.
Lokales Netzwerk (LAN)	Ein lokales Netzwerk verbindet lokale Endpunkte untereinander und ggf. über Zugangsnetze(n) mit Weitverkehrsnetz(en).
Local Internet Registry (LIR)	LIR: Lokale Organisation für das Management der Zuteilung und Registrierung von Internet-Ressourcen, u.a. Verwaltung von IP-Adressen (IPv4 und IPv6) sowie AS-Nummern Strategische LIR: Übernahme von strategischen Aufgaben durch BMI-Referat für Netze (aktuell: BMI CI 5) (z.B. Teilnahme an internationalen Konferenzen, Anregung von grundlegenden Policy-Änderungen im Eigeninteresse) Operative LIR: Übernahme von operativen Aufgaben durch BDBOS (z.B. Vergabe von Adressbereichen, Organisation von Schulungen für Sub LIR)

Begriff	Definition bzw. Erläuterung
Mandantenfähigkeit	Als mandantenfähig werden IT-Lösung bezeichnet, bei denen die Prozesse, Informationen und IT-Lösungen eines Auftraggebers strikt von denen anderer Auftraggeber getrennt sind, also keine Zugriffe oder Störungen von dem einen in den anderen Bereich möglich sind und somit auch deren Vertraulichkeit, Integrität oder Verfügbarkeit nicht beeinträchtigt werden kann.[82]
Netzdienstleistungen	Netzdienstleistungen sind die Gesamtheit organisatorischer, technischer und prozessualer Leistungen (u. a. netznahe und anwendernahe Dienste), die den Betrieb eines Netzes ermöglichen.
Kopplung (Netze)	Netzkopplung ist die Verbindung von Netzen. Die Netze bleiben mit ihren Attributen bestehen.
Netzbetreiber	Netzbetreiber bezeichnet eine Organisation, welche aus der Betreibersicht auf einen Netzverbund den Betrieb des Netzverbundes oder relevanter Teile des Netzverbundes verantwortet. In diesem Zusammenhang tritt ein Netzbetreiber nicht notwendigerweise als Netzdienstleister auf, da er in seiner Rolle als Betreiber eines Netzes nicht automatisch Nutzern Netzdienstleistungen anbietet bzw. erbringt. Dennoch geht die Rolle des/ der Netzbetreiberin im Hinblick auf Verantwortlichkeiten über die Rolle eines Anbieters hinaus.
Netzdienstleister	Netzdienstleister bezeichnet eine Organisation, welche aus Leistungssicht den Nutzern eines Netzverbundes Netzdienstleistungen anbietet.
Netzübergang	Ein Netzübergang ist die Schnittstelle zwischen gekoppelten Netzen, unter Berücksichtigung organisatorischer und sicherheitstechnischer Anforderungen und Attribute.
Netznahe Dienste	Dienste, die für den Betrieb eines Netzwerks zwingend erforderlich sind. Hierzu zählen z. B. Takt, PRC, SSU, NTP, DNS und DHCP. Für den Betrieb eines Netzverbunds, wie den IVÖV, sind netznahe Dienste zwingende Voraussetzung.
Nutzer	Als Nutzer werden Behörden und Einrichtungen verstanden, die Fachverfahren und Anwendungen bei den IT-Dienstleistern sowie Konnektivität bei der BDBOS nachfragen, um ihrem behördlichen oder ministeriellen Auftrag für die öffentliche Verwaltung nachzukommen. Neben den Nutzern (i. S. v. Einrichtungen bzw. Behörden) treten auch IT-Dienstleister als Nutzer insbesondere gegenüber der BDBOS auf, die diesen Netzdienstleistungen (bspw. netznahe Dienste (Protokolle), Konnektivität) bereitstellt.
Quality of Service (QoS)	Unter dem Begriff QoS werden alle Verfahren bezeichnet, die den Datenfluss in LANs und WANs so beeinflussen, dass der Dienst mit einer festgelegten Qualität beim Empfänger ankommt.
Sub Local Internet Registry (LIR)	Verantwortlichkeiten auf strategischer und operativer Ebene sind durch Entscheidung des IT-Planungsrates (Entscheidung 2016/43) bestimmt. Strategische Sub LIR: Eine strategische Sub LIR besitzt die Berechtigung, den allokierten Adressblock innerhalb ihres Zuständigkeitsbereiches eigenständig zu verwalten und / oder zu nutzen. Die Vergabe der Nutzungsrechte an strategische Sub LIRs wird von de.government koordiniert. Operative Sub LIR: Eine Sub LIR (z. B. ein Bundesland) kann die operative Verwaltung ihres Adressraums an eine operative Sub LIR übergeben (z.B. Hamburg an die operative Sub LIR (Dienstleister) Dataport). Die operative Sub LIR muss technisch und organisatorisch in der Lage sein, die operativen Sub LIR Aufgaben zu erfüllen. Die Adressraumberechtigung und Adressraumhoheit bleiben trotz der Übertragung weiterhin bei der strategischen Sub LIR.

[82] In Anlehnung an https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/glossar/04.html.

Begriff	Definition bzw. Erläuterung
Verbundene Netze	Zu den verbundenen Netzen im IVÖV gehören alle Netze, die über gesicherte Netzübergänge mit dem Basisnetz verbunden sind, um darüber Netzdienstleistungen der Anbieter von Leistungen im IVÖV zu nutzen oder in andere verbundene Netz zu kommunizieren.
Weitverkehrsnetz (WAN)	Ein Weitverkehrsnetz ist die Gesamtheit der vermittelnden Systeme und die Übertragungsstrecken zwischen LANs. Was ein vermittelndes System ist, ist auf jeder Netzebene unterschiedlich und muss im jeweiligen Kontext unterschieden werden.
Zulieferer	Unter Zulieferern werden die nachgelagerten, verwaltungsexternen (i. S. v. nicht-öffentlichen, da nicht im Eigentum der öffentlichen Verwaltung befindlich) Provider von Netzinfrastrukturen sowie Lieferanten und Hersteller von Systemtechnik und Software subsummiert.

Weitere nicht aufgeführte Begrifflichkeiten werden analog der Begriffsbestimmung im Projekt-Glossar der IT-Konsolidierung Bund sowie dem Glossar NdB 2019 verwendet.