Bundesministerium des Innern

Bericht der Bundesregierung zur

„Gesamtstrategie IT-Netze der öffentlichen Verwaltung“

Bericht für den Haushaltsausschuss zur strategischen Neuausrichtung der IT-Netze der öffentlichen Verwaltung

Inhalt

1. Auftrag

In der 63. Sitzung des HH-Ausschusses (HHA) am 21.09.11 wurde folgende Berichtsbitte beschlossen:

„Die Bundesregierung wird gebeten, dem Haushaltsausschuss bis zum 30.September 2012 zu berichten, wie die IT-Netze der öffentlichen Verwaltung strategisch so aufgestellt werden können, dass ihre Leistungsfähigkeit auch unter der verschärften Cybersicherheitslage dauerhaft gewährleistet werden kann. Dabei ist darzustellen, durch welche Betreibermodelle und Beschaffungsstrategien den gewachsenen Sicherheitsanforderungen sowie den Wirtschaftlichkeits- und Leistungsanforderungen Rechnung getragen werden kann.“

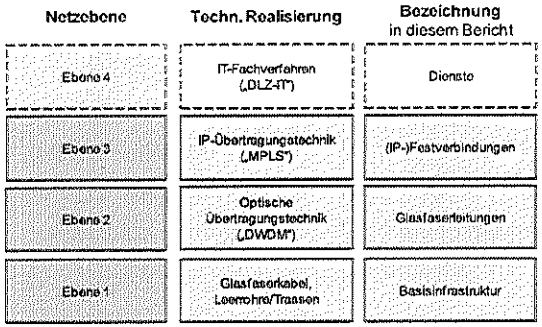
2. Betrachtungsgegenstand und Vorgehen

Betrachtungsgegenstand in diesem Bericht sind die Netze für IT- und Telekommunikation i. S. der für IT-Fachverfahren, Sprachvermittlung und Liegenschaftskopplungen sowie sonstiger Dienste notwendigen Weitverkehrsnetze.

Bei diesen Weitverkehrsnetzen (im Folgenden IT-Netze genannt) werden i. R. dieses Berichtes die Netzebenen:

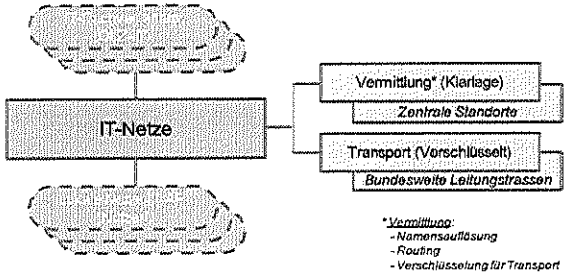
- Basisinfrastruktur i. S. von Glasfaserkabeln (einschl. Leerrohre hierfür und die dafür nötigen Trassen)
- Eigene oder angemietete Glasfaserleitungen mit optischer Übertragungstechnik
- Angemietete Festverbindungen z. B. mit IP-Übertragungstechnik (i. d. R. über Kupferleitungen)

getrennt betrachtet.



Ebenen und Technologien von IT-Netzen

Nicht betrachtet werden die IT-Fachverfahren (z. B. der DLZ-IT) selbst sowie die nutzerseitigen lokalen Netze (LAN) einschl. der IT-Arbeitsplätze.

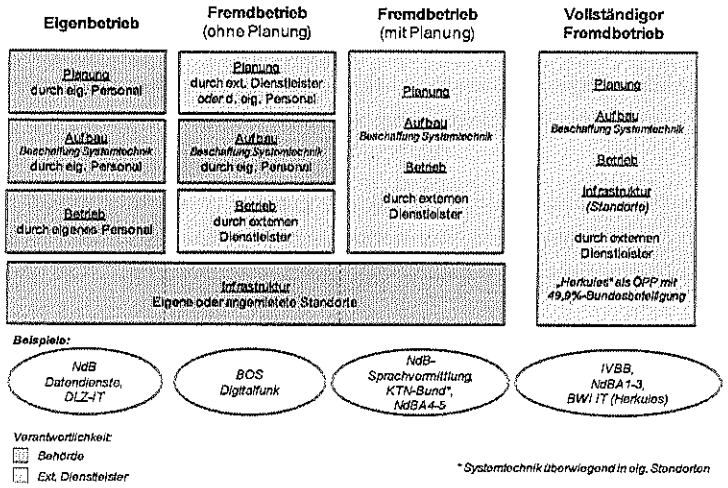


Betrachtungsgegenstand „IT-Netze“

Zu den IT-Netzen gehören neben den eigentlichen Übertragungswegen auch Dienste wie Netzverwaltung (Netz-Management, IT-Sicherheits-Management etc.) und häufig auch netznahe Datendienste (wie Verzeichnisdienst, Email-Gateway etc.), die jedoch als Teil des IT-Netzes hier nicht gesondert betrachtet werden, da ihre Realisierung i. d. R. als Teil des IT-Netzes oder der sonstigen Dienste erfolgt.

Bei den Betreibermodellen werden die Module Planung, Aufbau und Betrieb getrennt betrachtet, für die (bei einer konsequent angewendeten modularen Struktur der zu erledigenden Aufgaben) jeweils individuell entschieden werden kann,

mittels welcher Beschaffungsstrategie die einzelnen Module beschafft werden. Dabei ist u.a. auch zu berücksichtigen, in welchem Umfang in den jeweiligen Modulen die erforderlichen Leistungen durch Personal des Bundes erbracht werden können. Hierbei sind die jeweiligen Möglichkeiten von einer Erbringung aller Leistungen durch eigenes Personal und einer kompletten Leistungserbringung durch externe Dienstleister und diverse Mischformen hiervon, u.a. die Leistungserbringung im Rahmen einer öffentlich-privaten Partnerschaften (ÖPP) mit Beteiligung des Bundes, zu prüfen und zu bewerten.



Betreibermodelle mit Beispielen für deren Anwendung

Bei den Beschaffungen ist dabei zu unterscheiden zwischen:

(i) Vergabe von Lieferverträgen für technische Komponenten, Software etc. als Teil des Aufbaus dieser Technik (im Weiteren mit „Aufbau" bezeichnet)

(ii) Vergabe von Dienstleistungsverträgen an externe Dienstleister für Module wie Planung oder Betrieb,

wobei die Möglichkeit der Beauftragung externer Dienstleister vorab im Kontext der Sicherheitsanforderungen zu überprüfen ist.

Darüber hinaus ist anhand der ermittelten Sicherheitsbedarfe von Behördennetzen zu betrachten, inwieweit Aufbau und Betrieb dieser Technik in eigenen oder

angemieteten Räumlichkeiten stattfindet (mit „Infrastruktur" bezeichnet), um so eine uneingeschränkte Funktionsherrschaft der auftraggebenden Behörde zu realisieren.

Vorgehen

Im Vorfeld der Projekte „Netze des Bundes (NdB)" und „Deutschland Online Infrastruktur (DOI)" wurden 2007 umfassende Bestandsaufnahmen der IT-Netze in der Bundesverwaltung und im Bereich Bund-Länder-Kommunikation durchgeführt.

Diese Bestandsaufnahmen wurden i. R. dieser Berichterstattung durch 15 Interviews mit den spezifischen Fragestellungen dieses Berichtes aktualisiert:

- Berücksichtigung von parallel laufenden relevanten Vorhaben (z. B. IT-Konsolidierungen in den DLZ-IT) sowie neuen Möglichkeiten (z. B. Realisierung einer eigenen Transportnetz-Infrastruktur)
- Berücksichtigung Vorhaben anderer Ressorts
- Analyse und Bewertung unterschiedlicher Betreibermodelle und (daraus resultierende) Beschaffungsstrategien – insb. die Realisierung i. R. von ÖPP
- Sofern Informationen verfügbar und relevant: nationale und internationale Vergleiche und Analysen von Fallbeispielen für Ausbau und Betrieb von IT-Netzen.

Im Rahmen dieser Berichterstattung wurden folgende Gespräche und Interviews geführt:

- BDBOS (für Kerntransportnetz Bund)
- BMVg (für BWI-IT/Herkules)
- BVA/BIT (als DLZ-IT für den GB BMI)
- ZIVIT (als DLZ-IT für den GB BMF)
- BMVBS (für DLZ-IT BMVBS sowie den GB BMVBS mit den Netzinfrastrukturen von Straßenbau, Wasser-/Schifffahrtsverwaltung und Bahn)
- BA und DRV Bund im GB BMAS
- DOI (für das Bund-Länder-Verbindungsnetz)
- AA (für deren internationale Netze)
- Sicherheits-Behörden des BMI bzw. deren Fachaufsicht: BPol, BKA, BfV
- Fallstudien Inland: DFN Verein, Bahn, ARD.

Darüber hinaus stehen zusammen mit BMBF weitere Gespräche mit Forschungseinrichtungen wie Max Planck Gesellschaft, Fraunhofer Gesellschaft und Helmholtz-Gemeinschaft an.

3. Sachstand in der Bundesverwaltung

Sachstand „IST-Situation“

Es existieren heute in der Bundesverwaltung ca. 40 Weitverkehrsnetze, die in der Regel als IP-Mietleitungsnetze externer Dienstleister mit industrietypischer (und damit i. Vgl. zu Glasfasernetzen deutlich geringerer) Leistungsfähigkeit und Sicherheit ausgeführt sind.

Ausnahmen hiervon bilden die hochsicheren Hochleistungs-Backbone-Netze in Glasfasertechnik von BWI-IT („Herkules“), DWD (BVBS-WAN) sowie das im Aufbau befindliche Kerntransportnetz Bund („KTN-Bund“) für den Digitalfunk BOS und NdB, das in 2013 seinen Betrieb aufnehmen soll.

Im Projekt NdB werden neben dem Backbone-Netz (KTN-Bund) auch die Anbindungen von sicherheitskritischen Nutzern (wie heute schon im IVBB) und IT-Verfahrenszentren (z. B. die DLZ-IT) durch hochsichere Hochleistungsanbindungen in Glasfasertechnik realisiert.

In den Netzen, in denen weitergehende Sicherheitsanforderungen (z. B. Kryptierung) notwendig sind, werden diese Komponenten häufig im Eigenbetrieb der jeweiligen Behörde betrieben.

Aufgrund der vielen parallel betriebenen Netze existieren viele Verträge für Weitverkehrsdienstleistungen. Diese individuellen Verträge sind zeitlich (bzgl. Laufzeit und Vertragsende) sowie inhaltlich nicht synchronisiert. Verträge für Weitverkehrsdienstleistungen haben Volumina bis zu 40 Mio.€ p.a. (z. B. BA für IP-Festverbindungen).

Sachstand „Planung“

Zwischen BMI, BMVBS und BMF ist abgestimmt, dass mittelfristig für die Netze der Finanz- und Verkehrsverwaltung die Infrastruktur von NdB genutzt wird. Die Detailplanung hierzu ist noch nicht erarbeitet.

Zukünftig werden die Produkte und Services von NdB genutzt. Der konkrete Bedarf der DLZ-IT der GB BMI und BMVBS für deren Weitverkehrsnetze liegen derzeit noch nicht vor, da die dies bzgl. Planungen noch nicht abgeschlossen sind.
Im DLZ-IT im GB BMF sind die Planungen abgeschlossen und bereits umgesetzt: hier existiert ein hierarchisches Weitverkehrsnetz aus Backbone und Anschlussnetz auf Basis eines IP-Festverbindungsvertrages (hier: mit T-Systems).

BMVg erarbeitet derzeit die Planung zur Nachfolge BWI-IT (Herkules). Bzgl. der Mittel- und Langfristplanung für die Glasfasernetze von BWI-IT und KTN-Bund haben BMI und BMVg eine Zusammenarbeit vereinbart.

Neue Beschaffungen für Weitverkehrsdienstleistungen werden i. d. R. ausgelöst durch das jeweilige Ende der aktuellen Verträge. Typische Vertragslaufzeiten sind 4 oder 5 Jahre, jedoch existieren auch Verträge mit 10-jähriger Laufzeit.

Zusammenfassung

In der folgenden Tabelle sind die Ergebnisse der aktualisierten Bestandsaufnahme der Weitverkehrsnetze der Bundesverwaltung tabellarisch zusammengefasst.

Dabei ist zu berücksichtigen, dass eine solche Tabelle die einzelnen Netze nur bedingt vergleichbar darstellen kann, da es sich idR um unterschiedliche Lösungen für unterschiedliche Leistungs- und Sicherheitsanforderungen handelt.

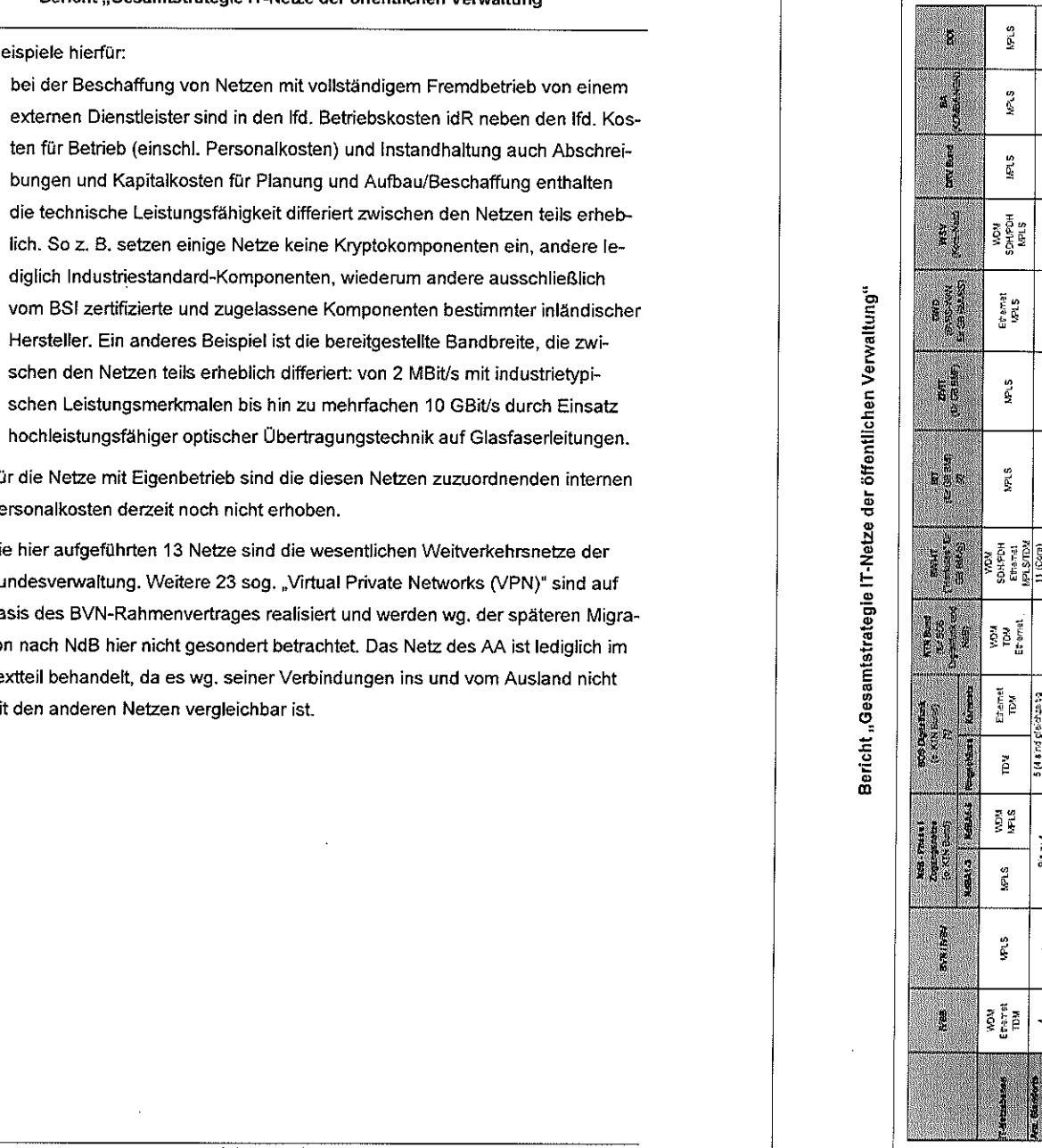
Insb. die Kostenangaben sind nur bedingt aussagefähig, da durch die unterschiedlichen Netz-, Betreiber- und Beschaffungskonzepte sowie unterschiedliche interne Kostenzuordnungen die jeweiligen Summen unterschiedliche Leistungen betreffen.

Beispiele hierfür:

- bei der Beschaffung von Netzen mit vollständigem Fremdbetrieb von einem externen Dienstleister sind in den lfd. Betriebskosten idR neben den lfd. Kosten für Betrieb (einschl. Personalkosten) und Instandhaltung auch Abschreibungen und Kapitalkosten für Planung und Aufbau/Beschaffung enthalten
- die technische Leistungsfähigkeit differiert zwischen den Netzen teils erheblich. So z. B. setzen einige Netze keine Kryptokomponenten ein, andere lediglich Industriestandard-Komponenten, wiederum andere ausschließlich vom BSI zertifizierte und zugelassene Komponenten bestimmter inländischer Hersteller. Ein anderes Beispiel ist die bereitgestellte Bandbreite, die zwischen den Netzen teils erheblich differiert: von 2 MBit/s mit industrietypischen Leistungsmerkmalen bis hin zu mehrfachen 10 GBit/s durch Einsatz hochleistungsfähiger optischer Übertragungstechnik auf Glasfaserleitungen.

Für die Netze mit Eigenbetrieb sind die diesen Netzen zuzuordnenden internen Personalkosten derzeit noch nicht erhoben.

Die hier aufgeführten 13 Netze sind die wesentlichen Weitverkehrsnetze der Bundesverwaltung. Weitere 23 sog. „Virtual Private Networks (VPN)" sind auf Basis des BVN-Rahmenvertrages realisiert und werden wg. der späteren Migration nach NdB hier nicht gesondert betrachtet. Das Netz des AA ist lediglich im Textteil behandelt, da es wg. seiner Verbindungen ins und vom Ausland nicht mit den anderen Netzen vergleichbar ist.



Übersicht „IT-Netze der öffentlichen Verwaltung“

Hinweise zur vorigen Tabelle:

- *MPLS steht hier für IP-Festverbindungsnetze. Für diese gilt grundsätzlich Fremdbetrieb, da sie von ext. Dienstleister als Gesamtdienstleitung mit industrietypischen Leistungsmerkmalen bereitgestellt werden. Ausnahme hiervon ist z. B. das MPLS-Netz im BVBS-WAN, das im Eigenbetrieb betrieben wird.*
- *TDM und SDH/PDH stehen für sonstige nicht IP-basierte, leitungsvermittelnde Übertragungstechniken*
- *WDM steht hier für optische Übertragungstechnik auf Glasfaserleitungen (CWDM oder DWDM)*
- *Standorte i. S. von Großräumen (z. B. BA mit 2 RZ in Nürnberg = 1 Standort).*

Anmerkungen in der Tabelle:

[1] Betrachtung begrenzt auf die Digitalfunk-Festnetzbereiche, die möglichen Netzkonsolidierungen im Sinne einer gemeinsamen IT-Strategie unterliegen (Festnetzverbindungen zwischen Kernnetzstandorten des Digitalfunks BOS)

[2] GB ohne Sicherheitsbehörden

[3] Hier Liegenschaften die an das Weitverkehrsnetz angeschlossen sind (Daten- und/oder Sprache)

[4] Daten und Sprache (140.000 APC, 11.000 Drucker, 280.000 TK-Endgeräte, 30.000 Nutzer in militärischen Systemen)

[5] Industriestandard-Kryptierung ohne BSI-Zulassung (z. B. CISCO GetVPN)

[6] Verträge für Weitverkehrsdienstleistungen (keine Betrachtung von Dienston i. S. dieses Berichtes)

[7] Ablösung durch NdB-Phase I: NdB-Anschlüsse 1-3

[8] Ablösung durch NdB-Phase I: NdB-Anschlüsse 4-5

[9] Gem. NdB-Bestandsaufnahme von 2008 mit Aktualisierung in Feb. 2012 ("HH-begründende Unterlage 2013"; hierbei sind auch die WAN-Kosten für die o.g. 23 VPN berücksichtigt

10] Einmalkosten (ggf. als Investitionen) nur für erstmalige Migration von Altnetzen erforderlich; idR nicht für Folgeverträge

[11] Kalkulatorisch, bei vollständiger Umsetzung

[12] Geplanter Betriebsbeginn: Dez. 2013

[13] Kosten einschl. Investitionen sowie lfd. Kosten für Infrastruktur, Carrier-Dienstleistungen und Personal

[14] DRV Bund ist Nutzer des Weitverkehrsnetzwerks (WAN) der gesamten DRV. Eine Kosten- und Leistungsrechnung für die DRV befindet sich zurzeit im Aufbau. Insofern können hier keine belastbaren Zahlen genannt werden.

[15] Gesamtkosten für Bund und Länder in 2013

[16] Für BSI-zugelassene Kryptotechnik

[17] Beispiel BAMF: lfd. Kosten 1,3 Mio.€/a für 28 Standorte mit Bandbreitenbedarf von 2 MBit/s (Externer Dienstleister: T-Systems)

Im Folgenden werden IST-Situation (mit Leistungsumfang einschl. Sicherheitsanforderungen, Betreibermodell und Beschaffungsstrategie) sowie Planungen (sofern wesentliche Veränderungen geplant sind) der Netzaktivitäten zusammenfassend beschrieben von:

- Projekt „Netzes des Bundes“
- BOS Digitalfunknetz und KTN-Bund (BDBOS)
- Deutschland Online Infrastruktur (DOI)
- BMVg für BWI-IT („Herkules“)
- Angebot einer bundeweiten Glasfaser-/Leerrohrinfrastruktur
- BMI für BVA/BIT als DLZ-IT im GB des BMI
- BMF für ZIVIT als DLZ-IT im GB des BMF
- BMVBS für DLZ-IT BMVBS, DWD und WSV (ohne Bahn)
- BA
- DRV Bund
- sowie AA.

3.1 Netze des Bundes

Sachstand: IST-Situation

Leistungsumfang

Der derzeitige Projektauftrag des Projektes NdB umfasst den Ersatz der beiden ressortübergreifenden Netze IVBB und IVBV/BVN für ca. 700 Nutzerliegenschaften mit ca. 80.000 Teilnehmern mit dem durchgängigen Sicherheitsniveau des heutigen IVBB (Schutzbedarf „hoch“ / VS-NfD).

Ziel ist die Bereitstellung der Transportebene für eine durchgängige, einheitliche, standortunabhängige (bundesweite) und an den Anforderungen der Fachaufgaben ausgerichteten Netzinfrastruktur für Sprach- und Datenkommunikation für die Bundesverwaltung (einschl. netznaher Dienste). Die NdB-Infrastruktur wird es ermöglichen, allen NdB-Nutzern IT-Fachverfahren über eine standardisierte Schnittstelle bundesweit und hochsicher (verfügbar, vertraulich, integer) bereitzustellen.

Auf diesem Funktionsumfang und Mengengerüst (mit einer Topologie von drei geo-redundanten Netzverwaltungszentren und insgesamt drei zusätzlichen Knotenvermittlungen) basieren die Anforderungen von NdB an das in Realisierung befindliche KTN-Bund.

Neben dem KTN-Bund existieren hochsichere und hochperformante Anschlüsse für Nutzer und IT-Verfahrenszentren als Glasfaserleitungen. Die sonstigen Nutzeranschlüsse werden als IP-Mietleitungen eines ext. Dienstleisters realisiert.

Betreibermodell

NdB ist i. W. modular strukturiert (Trennung von Planung, Beschaffung und Betrieb bei Nutzung eigener Infrastruktur für die zentralen Standorte). Dadurch kann je nach Komplexität, bestehenden Sicherheitsanforderungen und eigener Leistungsfähigkeit für jede bereitzustellende Funktion zwischen Eigenbetrieb oder Vergabe an einen ext. Dienstleister entschieden werden.

Der Aufbau von NdB ist für folgende Funktionsbereiche durchgängig modular:

- Zentrale Serviceorganisation (ZSO) als Schnittstelle zum Nutzer und für die Steuerung und Koordinierung von Prozessen sowie externen Dienstleistern
- IT-Sicherheitsmanagement gemäß UP Bund (Unterstützung durch BSI)
- Netzverwaltung mit Logik- und Vermittlungsbereichen („Kernbereich“)
- Netznahe Datendienste (z. B. Vz-Dienst, IAM, E-Mail-Gateway)
- Sprachdienste (Sprachvermittlung, Videokonferenz sowie UMS)
- KTN-Bund als zentrales Architekturelement für Verfügbarkeit und Krisensicherheit (Realisierung zusammen mit BDBOS, Nutzung durch NdB und BOS Digitalfunk)
- Bundesweite Nutzeranbindungen als Glasfaser- oder IP-Festverbindungen.

Die Systemtechnik wird in drei eigenen geo-redundanten Netzverwaltungszentren (NVZ) aufgebaut und betrieben.

Für die Funktionsbereiche Kernbereich und Datendienste ist Eigenbetrieb geplant. Die Funktionsbereiche Sprachvermittlung, NdBA5-Zugangsnetz und KTN-Bund werden aufgrund fehlender eigener Leistungsfähigkeit oder eigener Infrastruktur unter Berücksichtigung der hohen Sicherheitsanforderungen durch vertrauenswürdige externe Dienstleister erbracht.

Aufbau/Beschaffung

Die aus dem modularen Ansatz resultierenden Vergaben reichen von der Beschaffung notwendiger Systemtechnik (z.B. Netzwerkkomponenten oder Sicherheitstechnik wie Verschlüsselungsgeräte) bis hin zu Vergaben für die Realisierung und den Betrieb ganzer Module (z.B. Zugangsnetze für die Anschlüsse der Nutzer). Die einzelnen Vergaben sind so gestaltet, dass insbesondere sicherheitskritische Bereiche gesondert vergeben werden können.

Sachstand – Planung

Nach Abschluss der derzeitigen Ausbauphase soll die Konsolidierung der IT-Netze der Geschäftsbereiche von BMI, BMF und BMVBS sowie DOI geplant und umgesetzt werden.

Die zukünftige Konsolidierung weiterer großer Netze wie die von BA und DRV Bund ist derzeit noch offen.

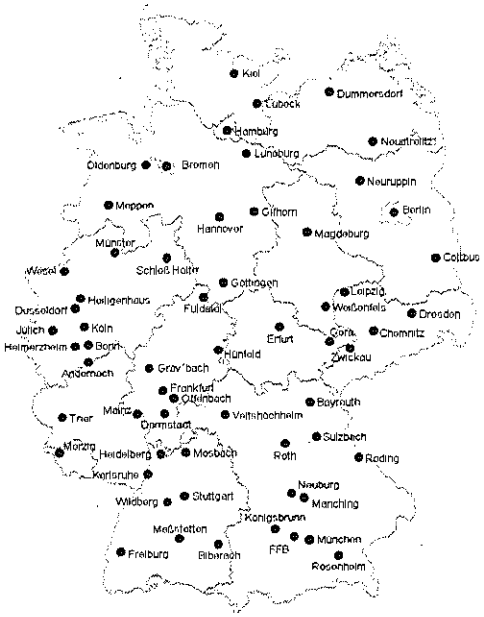
3.2 BOS Digitalfunknetz und KTN-Bund (BDBOS)

Sachstand – IST-Situation

Leistungsumfang/Aufgabenstellung

Zentrale Aufgaben der BDBOS sind Aufbau und Betrieb eines professionellen, bundesweiten Funknetzes für die BOS auf Basis des TETRA-Standards. Darüber hinaus hat die BDBOS die Federführung für das derzeit gemeinsam mit NdB in Realisierung befindliche Kerntransportnetz des Bundes (KTN-Bund) als bundesweites Hochleistungs-Glasfasernetz mit optischer Übertragungstechnik („DWDM“).

Die KTN-Bund-Systemtechnik wird in insges. 63 Kernnetzstandorten des Digitalfunks (DWDM und zusätzliche Technik für die leitungsvermittelten Netze des Digitalfunks) sowie 4 exklusiven NdB-Standorten (nur DWDM) realisiert. Zudem nutzt NdB 2 Digitalfunkstandorte als Knotenvermittlungen für seine Zugangsnetze. Das KTN-Bund soll im Dezember 2013 den Wirkbetrieb aufnehmen.



Städte mit „Kerntransportnetz Bund“-Knoten

Betreibermodell

Die Kernaufgaben der BDBOS, bestehend aus Planung, Lieferung/Aufbau (Beschaffung) und Betrieb der Digitalfunk-Systemtechnik sowie Projektsteuerung und –controlling, sind modular strukturiert. Aufbau und Betrieb der Systemtechnik erfolgen in eigenen Standorten.

Das KTN-Bund ist aus Sicherheitsgründen nicht-modular strukturiert, es wird durch einen Generalunternehmer, die T-Systems, realisiert.

Planung/Aufbau/Betrieb

Für den Digitalfunk bedient sich BDBOS externer Unterstützung für die Module Planung, Lieferung/Aufbau und Betrieb.

KTN-Bund wurde aus Sicherheitsgründen an den vertrauenswürdigen externen Dienstleister T-Systems vergeben. Ein Eigenbetrieb der gesamten Systemtechnik ist durch die Überleitungsklausel im KTN-Bund-Vertrag gesichert.

3.3 DOI

Sachstand – IST-Situation

Leistungsumfang/Aufgabenstellung

Im Rahmen des Vorhabens „Deutschland Online Infrastruktur (DOI)“ wurde 2009 ein Netz aufgebaut, das die deutschen Verwaltungsnetze von Bund, Ländern und Kommunen flächendeckend miteinander verbindet. Es wird als „Verbindungsnetz“ gemäß Ausführungsgesetz zu Art. 91c Absatz 4 GG („Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder (IT-NetzG)“) vom Bund betrieben.

Das DOI-Netz verbindet momentan 80 Nutzer aus Bund, Ländern und Kommunen mit ca. 110 Liegenschaften und den dahinterliegenden Netzen. Die derzeitig angebotene maximale Bandbreite beträgt 2,5 GBit/s.

DOI hat den Schutzbedarf hoch und ist vom BSI entsprechend zertifiziert.

Betreibermodell, Aufbau/Beschaffung

Der derzeitige DOI-Vertrag für Weitverkehrsdienstleistungen wurde i. R. einer wettbewerblichen Ausschreibung vergeben (derzeit T-Systems). Der Vertrag läuft im März 2014 (nach einmaliger Verlängerung) aus und kann noch einmal um 1 Jahr verlängert werden, so dass spätestens im März 2015 mit der Migration der jetzigen Anschlüsse begonnen werden muss, die spätestens im März 2016 beendet sein muss.

Sachstand - Planung

Laut § 3 IT-NetzG, der zum 1. Januar 2015 in Kraft tritt, erfolgt der Datenaustausch zwischen dem Bund und den Ländern (ausschließlich) über das Verbindungsnetz. Zur Umsetzung dieser gesetzlichen Vorgabe müssen parallel zu den oben dargestellten Aktivitäten die weiteren Netzinfrastrukturen identifiziert werden, die für den Datenaustausch zwischen Bund und Ländern genutzt werden.

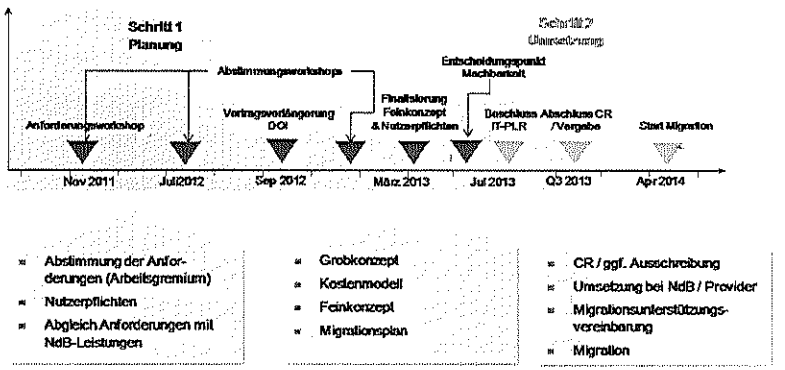
In einem zweiten Schritt müssen die Anforderungen an diese Netze aufgenommen werden, um das Verbindungsnetz im Sinne des § 3 IT-NetzG in Zukunft auch für diesen Datenaustausch bereit stellen zu können.

Zur Realisierung einer Nachfolgelösung einschl. des Bund-Länder-Verbindungsnetzes gem. § 3 IT-NetzG wurde von Bund (BMI) und Ländern ein Projekt mit folgenden Aufgaben etabliert:

- Analyse und Abstimmung der Anforderungen mit Ländern und Kommunen auf politisch-strategischer Ebene sowie mit NdB
- Analyse der Anforderungen in Bezug auf Funktionalität, Architektur, Betrieb und Wirtschaftlichkeit
- Beschreibung und Bewertung der fachlichen, organisatorischen und ökonomischen Optionen mit dem Ziel, die hochsichere NdB-Infrastruktur als Basis für das zukünftige Verbindungsnetz zu nutzen (s. a. Anhang A.3 IT-Staatsvertrag[1])
- Erstellung eines abgestimmten Projektplans.

Bis Anfang 2014 ist eine Entscheidung bzgl. des weiteren Vorgehens (Neuausschreibung oder Migration auf NdB) erforderlich. Mittelfristig ist eine Konsolidierung mit NdB vorgesehen.

[1] *„Der Bund betreibt gegenwärtig die Neugestaltung seiner IT-Netze in einer modularen Architektur und auf der Grundlage eines Transportnetzes auf Basis von Dark Fibre. Dies geschieht in ausschließlicher Zuständigkeit des Bundes. Unter Nutzung des Transportnetzes dieser ohnehin im Aufbau befindlichen bundesweiten IT-Netzinfrastruktur kann das Verbindungsnetz als eigenes VPN (einschließlich Zugangsnetz) realisiert werden. Möglich ist außerdem die optionale Nutzung von Diensten aus dem Portfolio (Warenkorb) des Projektes „Netze des Bundes““.*



Zeitplan Nachfolge DOI/Verbindungsnetz

3.4 BMVg

Sachstand – IST-Situation

Leistungsumfang/Aufgabenstellung

Die IT-Aktivitäten des BMVg sind weitgehend in der BWI Informationstechnik GmbH (BWI-IT) gebündelt.

Die Kernaufgaben der BWI-IT sind mit Blick auf IT-Vernetzung:

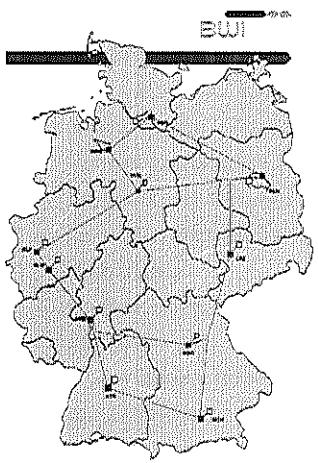
- Planung, Beschaffung und Betrieb eines modernen, hochsicheren Weitverkehrsnetzes der Bundeswehr (WANBw) zwischen bundesweit insges. 1.245 Liegenschaften mit einer Backbone-Struktur zwischen 11 zentralen Standorten (s. u. Abb. „BWI IT Backbone-Kernnetze“)
- Planung, Beschaffung und Betrieb der lokalen Netze (LAN) in den 1.245 Liegenschaften
- Planung, Beschaffung und Betrieb der derzeit 140.000 IT-Arbeitsplätze (AP) inklusive eines zentralen UHD
- Planung, Beschaffung und Betrieb der Telekommunikationsanlagen in den Liegenschaften mit derzeit 280.000 Telefonen (teilweise mit IP-Telefonie) inklusive eines zentralen Auskunfts- und Vermittlungsdienstes sowie den Übergängen ins öffentliche Telefonnetz

- Bereitstellung eines Zugangs der Auslands- und Einsatzstandorte sowie der seegehenden Einheiten der Marine zum WANBw in Strausberg und Köln
- Anbindung an das öffentliche Internet in Strausberg und Köln
- Anbindung von ca. 6.200 mobilen Arbeitsplätzen (einschl. Telearbeitsplätze)
- Planung, Beschaffung und Betrieb der Zentralen Dienste (Internet, Intranet, E-Mail, PKI) in drei Rechenzentren
- Überwachung und Steuerung aller AP, Netze und Dienste durch Betriebs-/ Kompetenzzentren im Inland.

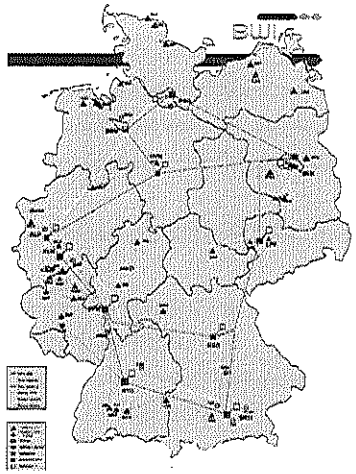
Weitverkehrsinfrastruktur

Bzgl. der IT-Netze als Betrachtungsgegenstand dieses Berichtes ist die Situation in der Bundeswehr im Inland wie folgt:

- BWI-IT betreibt ein Weitverkehrsnetz auf Basis angemieteter Übertragungswege („unbeleuchteter“ Glasfasern) im Wesentlichen mit optischer Übertragungstechnik (DWDM). Die Übertragungswege des Kernnetz sind weitgehend redundant ausgelegt, um so die geforderte Verfügbarkeit zu erreichen
- Dazu sind auf der untersten Netzebene im Backbone und den Sub-Ringen zu den Kernstandorten u.a. die Übertragungswege bei unterschiedlichen Carriern angemietet. Für diese Übertragungswege nutzt die BWI IT Leitungen von drei Carriern (GasLINE, Interroute und KPN)
  Anmerkung: die Telekom bietet Endkunden insb. aus regulatorischen Gründen weiterhin keine „unbeleuchteten“ Glasfasern an
- BWI-IT hat dieses Weitverkehrsnetz geplant, beschafft und betreibt es auch
- Transportdienste anderer bundeseigener Netze (z. B. dem Kerntransportnetz Bund von BDBOS und NdB) können aus Gründen der unterschiedlichen Architekturansätze derzeit nicht genutzt werden. Eine Nutzung ist daher i. R. des derzeitigen BWI-IT Aufgabenumfanges auch nicht geplant.
  Neben den direkt an NdB angeschlossenen Liegenschaften BMVg Bonn und Berlin sowie MAD Amt Köln wird ein redundant ausgelegter transparenter Zugang zu ausgewählten Diensten von NdB, wie z.B. zum Intranet des Bundes realisiert (heute über einen transparenten IVBV/BVN-Zugang realisiert).



BWI IT „Backbone“-Kernnetz



BWI IT 22 „Top 50“-Liegenschaften

Sicherheitsanforderungen

Die sicherheitstechnischen Anforderungen des BMVg bzgl. Verfügbarkeit, Vertraulichkeit und Integrität sowie Verbindlichkeit werden durch die im Hauptvertrag HERKULES vereinbarten Leistungsverpflichtungen abgedeckt.

Die Anforderungen des BMVg an die Vertrauenswürdigkeit externer Dienstleister werden durch die Geheimschutzbetreuung der Wirtschaft durch das BMWi erfüllt. Bezüglich der eingesetzten technischen Komponenten des WANBw werden die Zulieferer der Komponenten regelmäßig kontrolliert, um eine vertrauenswürdige Logistikkette vom Hersteller zur BWI aufzubauen. Eine Trennung zwischen Daten und Sprache findet auf Ebene der Netzkomponenten, nicht jedoch durch physikalisch getrennte Netze statt.

Betreibermodell & Beschaffung

In der BWI-IT sind sowohl Planung, Beschaffung und Betrieb gebündelt. Die bereitzustellenden Leistungen sind vertraglich mit BMVg vereinbart.

Die BWI-IT ist eine Öffentlich-Private-Partnerschaft (ÖPP), deren privatwirtschaftliche Anteile nach Ausschreibung in 2006 vergeben wurden. Die dies

bzgl. Verträge haben eine Laufzeit von 10 Jahren und laufen Ende Dezember 2016 aus.

Der Bund hält 49,9 % der Anteile an der BWI-IT. Die unternehmerische Steuerung seitens der Bundeswehr obliegt ihren Vertretern in den Organen der Gesellschaft. Das Auftraggeber-Management nimmt das BAAINBw wahr. Durch die Struktur als ÖPP hat die Bundesrepublik Deutschland als Anteilseigner vertreten durch das BMVg Einflussmöglichkeiten auf unternehmerische Entscheidungen der BWI-IT.

Über den Hauptvertrag HERKULES hinaus verfügt Bundeswehr über weitere Verträge mit externen Dienstleistern z. B. für spezifische IT-Leistungen wie Satellitenkommunikation und terrestrische Leitungen (insbesondere im Ausland).

Sachstand - Planung

Für die Folgelösung ab 2017 nach Auslaufen der BWI-IT Verträge wird BMVg dem Haushaltsausschuss zum weiteren Vorgehen auf Basis einer Wirtschaftlichkeitsuntersuchung bis Ende 2013 berichten. Hierzu sind folgende Meilensteine geplant:

- Analyse und Bewertung von Alternativen zu Organisationsmodellen (von Eigenbetrieb über die formelle bis hin zur funktionalen Privatisierung)
- Erstellung eines Leistungskataloges für die Bedarfsdeckung. Dabei soll, falls möglich, auch der Bedarf anderer Ressorts und die angebotenen Dienstleistungen - insb. der zwischenzeitlich etablierten Dienstleistungszentren (DLZ-IT) von BMI, BMF und BMVBS - berücksichtigt werden.

Im Rahmen der weiteren Planung der Herkules-Folgelösung ab 2017 wird eine wechselweise Nutzung der Kapazitäten des Kerntransportnetzes der Bundeswehr und des Kerntransportnetzes Bund von BDBOS und NdB geprüft.

Ein mögliches Ergebnis könnte die Reduktion von derzeit zwei auf eine bundesweite Kerntransportnetzinfrastruktur sein.

3.5 Angebot einer bundeweiten Glasfaser-/Leerrohrinfrastruktur

Sachstand – IST-Situation

Dem BMI liegt ein Angebot zum Kauf einer bundesweiten dedizierten Leerrohrinfrastruktur von ca. 4.000 km Länge vor, die bereits in Teilen mit Glasfaserkabeln ausgestattet ist bzw. kurzfristig ausgerüstet werden kann.

Der für die IT-Nutzung notwendige Aufbau der optischen Übertragungstechnik („DWDM“) ist noch nicht erfolgt und wird dem Erwerber überlassen, so dass eine modulare Struktur (getrennte Realisierung von Planung, Aufbau und Betrieb) möglich ist.

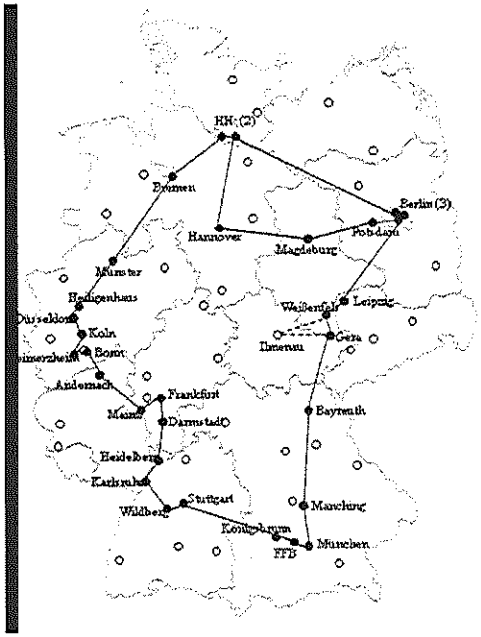
Das Angebot beinhaltet den Kauf der installierten Infrastruktur (i. W. Leerrohre, Kabelschächte und die bereits verlegten Glaserkabel) sowie die Trassenrechte einschl. Dokumentation.

Nach derzeitiger Einschätzung erreicht diese Infrastruktur (erweitert um die notwendigen lokalen Liegenschaftsanschlüsse) alle zentralen Standorte von NdB, aller DLZ-IT sowie des heutigen BMVg-Backbone-Netzes. Daneben werden 11 der 16 Landeshauptstädte erreicht.

Neben den Anforderungen an die Topologie erfüllt diese Infrastruktur nach erster Einschätzung insb. die Anforderungen an heutige und zukünftige Leistungsfähigkeit, Sicherheit (insbesondere an die uneingeschränkte Funktionshoheit des Bundes), Wirtschaftlichkeit und Realisierbarkeit. Der Bund würde über ein zukunftsfähiges Netz mit fast beliebiger Bandbreite verfügen, auf dem auch zukünftige, bandbreitenintensive Dienste verschiedener Nutzer abgebildet (z.B. Bildübertragung von Videokameras) bzw. neue Nutzer und Nutzergruppen (Konsolidierung von Verwaltungsnetzen) integriert werden können. Die angebotene Infrastruktur wurde nach militärischen Vorgaben geplant und errichtet, die zum Teil sogar die Forderungen von „Netze des Bundes“ übersteigen. Probleme, die bei Anmietung solcher Strukturen i.d.R. bestehen (z.B. Mitnutzer der Glasfaserkabel etc.), würden hier nicht auftreten.

Diese Struktur kann mindestens in Teilen eine Ergänzung zu den angemieteten Glasfasern darstellen. Hieraus könnten sich Synergien aus Eigenverantwortung für Infrastrukturelemente und Flexibilität einer Marktversorgung ergeben. Dies bedarf jedoch einer detaillierten Untersuchung.

Damit kann diese Infrastruktur mittelfristig das zentrale Element einer hochsicheren (dedizierten) und hochleistungsfähigen (hoch skalierbaren) Regierungskommunikation für Bund und Länder werden.



Mögliche Zieltopologie für die Transportnetzinfrastruktur

Der Erwerb dieser Infrastruktur wird zwar **nicht zum Nulltarif** erfolgen können, erscheint aber aufgrund einer ersten und noch zu verifizierenden Einschätzung für den Bund langfristig wirtschaftlich bei gleichzeitig erheblicher Steigerung von Leistungsfähigkeit (insb. im Hinblick auf Skalierbarkeit/Zukunftssicherheit) und IT-Sicherheit (als robuste dedizierte Basisinfrastruktur).

Sachstand – Planung

Die endgültige Kaufentscheidung hängt u. a. davon ab, inwieweit diese Infrastruktur bereits mittelfristig in die Weiterentwicklung der verschiedenen Bundesnetze eingebunden werden kann.

Zur Vorbereitung einer Kaufentscheidung wäre über die bisherigen Bewertungen des Angebotes hinaus zusammen mit dem Verkäufer eine detaillierte Sachstands- und Risikoanalyse („Due Diligence“) zu erarbeiten.

DLZ-IT

Betrachtet werden im Folgenden die Planungen von BMI, BMF und BMVBS bzgl. ihrer jeweiligen DLZ-IT-Aktivitäten. BWI-IT als DLZ-IT im Geschäftsbereich des BMVg ist Teil der Mittel- und Langfristplanung von BMVg und wird hier nicht gesondert betrachtet.

3.6 BVA/BIT als DLZ-IT im Geschäftsbereich des BMI

Sachstand – IST-Situation

Leistungsumfang/Aufgabenstellung

Die Bundesstelle für Informationstechnik (BIT) ist zentraler IT-Dienstleiter der Bundesverwaltung und zuständig für die IT-Konsolidierung im Geschäftsbereich BMI (ohne Sicherheitsbehörden). Darüber hinaus bietet die BIT auch Dienstleistungen für Kunden außerhalb des GB an.

Derzeit nutzt BVA/BIT die bestehenden ressortübergreifenden Netze (IVBB, IVBV/ BVN sowie DOI) und betreibt keine eigenen IT-Weitverkehrsinfrastrukturen. Ein besonderer Schwerpunkt bzgl. Verfügbarkeit wird dabei auf die Anbindung der Rechenzentren untereinander gelegt.

Schutzbedarf besteht bis „hoch“ (nicht durchgängig VS NfD).

Aktuell wird im Zuge der Konsolidierung im GB BMI ein Konzept erarbeitet, in dem u. a. die Anforderungen der zu konsolidierenden Behörden (wie z. B. BAMF) an das konsolidierte Weitverkehrsnetz ermittelt werden. Die heutigen individuellen Weitverkehrsnetze im GB BMI werden künftig durch NdB abgelöst.

Betreibermodell

Derzeit betreibt BVA/BIT kein eigenes Netz, sondern greift auf die derzeitigen ressortübergreifenden Netze wie IVBB, DOI sowie zukünftig NdB zurück. Hier ist auch zukünftig keine Änderung vorgesehen.

Aufbau/Beschaffung

Aufgrund der vorgesehenen Nutzung von NdB sind eigene Beschaffungsmaßnahmen für Weitverkehrsnetze von BVA/BIT nicht geplant.

Sachstand – Planung

Mit ersten Ergebnissen der Bestandserhebungen wird in 2013 gerechnet. Folgende Maßnahmen sollen daraufhin ergriffen werden:

- Konsolidierung aller IT-Verfahren in die Rechenzentren Köln und Wiesbaden
- Hochperformante Anbindung dieser RZ untereinander nach konkretem Bedarf
- Anbindung der Nutzerliegenschaften an die IT-Verfahren in diesen RZ mit einer Skalierbarkeit der Weitverkehrsnetze von mind. 10 GBit/s auf Verfahrensseite
- Administration aller zentralen und dezentralen IT-Komponenten im GB.

Notwendig ist darüber hinaus auch die Anbindung der zu konsolidierenden RZ im GB BMI für den Zeitraum der Migration in die RZ in Köln und Wiesbaden.

3.7 ZIVIT als DLZ-IT im Geschäftsbereich des BMF

Sachstand – IST-Situation

Leistungsumfang/Aufgabenstellung

Das Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT) ist zentraler IT-Dienstleister für den GB BMF und bietet IT-Dienstleistungen auch für Kunden außerhalb des GB BMF in der Bundesverwaltung und zum Teil in den Bundesländern an.

ZIVIT betreibt als DLZ-IT im Geschäftsbereich des BMF das Weitverkehrsnetz der Bundesfinanz-Verwaltung (BFV-WAN) mit einer hierarchischen Struktur aus Backbone- und Accessnetz. Netzübergänge existieren z. B. zu IVBB, IVBV/BVN, DOI und dem öffentlichen Internet.

Die etwa 1.100 Nutzer-Standorte mit ca. 50.000 Teilnehmern sind über ein IP-Mietleitungsnetz eines ext. DL (hier: T-Systems) angeschlossen.

Das BFV-Netz hat den Schutzbedarf „hoch“ (VS-NfD) mit entspr. gesicherten Netzzugängen und unterschiedlichen Geschwindigkeiten und Verfügbarkeitsklassen. Die Verschlüsselung des Backbone erfolgt mit von BSI zugelassenen Krypto-Boxen (Layer 2: Atmedia/Secunet, Layer 3: Genua).

Betreibermodell

Das BFV-Netz ist (ähnlich NdB) modular aufgebaut. Die gesamte Switch- und Sicherheitstechnik ist im Besitz des ZIVIT.

Grundsätzlich erfolgt ein Eigenbetrieb der Rechenzentren. Ausnahme hiervon ist das IP-Mietleitungsnetzes mit Fremdbetrieb durch den ext. DL. Hier ist kein Eigenbetrieb möglich. Der Betrieb von sicherheitskritischen Aufgaben wie Routing und Betrieb der Krypto-Technik für dieses IP-Mietleitungsnetz findet jedoch im Eigenbetrieb statt.

Aufbau/Beschaffung

IP-Mietleitungen werden durch einen ext. DL bereitgestellt (derzeit T-Systems).

Die Kosten des Netzes betragen ca. 25 Mio.€ p. a.

Der aktuelle Vertrag endet 2013.

Sachstand – Planung

Eine Hochrüstung des Backbones auf 1GBit/s ist in 2013 geplant. Da das Netz bereits VS-NfD verschlüsselt ist, sind weitere Maßnahmen derzeit nicht geplant.

3.8 DLZ-IT BMVBS als DLZ-IT im Geschäftsbereich des BMVBS mit DWD und WSV

Im BMVBS gibt es zwei IT-Weitverkehrsnetze:

- das Weitverkehrsnetz der Bundesverwaltung für Verkehr, Bau und Stadtentwicklung (BVBS WAN) wird vom Deutschen Wetterdienst (DWD) bereitgestellt („trockener Bereich“)
- die Wasser- und Schifffahrtverwaltung (WSV) betreibt i. R. ihrer Betriebsaufgaben in Ergänzung zum BVBS-WAN eine eigene Netzinfrastruktur aus Glasfaserleitungen und Richtfunkstrecken („nasser Bereich“).

Deutscher Wetterdienst (DWD)

Sachstand – IST-Situation

Leistungsumfang/Aufgabenstellung

- Bereitstellung einer dienste-neutralen Hochleistungs-Kommunikationsinfrastruktur einschließlich zentraler Kommunikationsdienste für alle Fachaufgaben des GB des BMVBS.
- Hierarchisches Weitverkehrsnetz mit Backbone (Glasfaserverbindungen mit je 2x1 GBit/s) und sternförmigen Anbindungen von ca. 400 Nutzerstandorten mit ca. 25.000 Teilnehmern (Layer 3 mit bis zu 1 GBit/s) jeweils als IP-Mietleitungen.

Der Schutzbedarf ist „normal“.

Betreibermodell

Modulare Struktur für Planung, Aufbau (i. S. Beschaffung Systemtechnik) und Betrieb mit umfänglichem Eigenbetrieb.

Aufbau/Beschaffung

Beschaffung von Weitverkehrsdienstleistungen (außerhalb des Glasfaser-Backbone-Netzes) erfolgt durch:

- Festverbindungen durch wettbewerbliche Vergabe am Markt (der IP-Layer wird durch DWD realisiert)
- Glasfaserleitungen von der WSV.

Der Vertrag für das IP-Mietleitungsnetz (derzeit T-Systems) hat eine Laufzeit von 4 Jahren. Nach Ablauf erfolgt eine erneute EU-weite Ausschreibung.
Die derzeitigen Kosten belaufen sich auf ca. 5 Mio.€ p.a.

Sachstand – Planung

Grundsätzliche andere Anforderungen an Leistungsfähigkeit, Betreibermodell und Beschaffungsstrategien sind derzeit nicht absehbar. Bzgl. der Übertragungsraten werden allerdings erhebliche Wachstumsraten erwartet.

Wasser- und Schifffahrtsverwaltung (WSV)

Sachstand – IST-Situation

Leistungsumfang/Aufgabenstellung

- Bereitstellung des Betriebsnetzes für Wasserstraßen einschl. Schleusensteuerung und Wasserstaßenfunk
- Eigene Glasfaser- und Kupferkabel sowie Richtfunkstrecken mit bis zu 600 MBit/s in und an Bundeswasserstraßen (380 Standorte für Übertragungstechnik)
- Hierarchisches Weitverkehrsnetz mit sternförmigen Anbindungen von ca. 250 Nutzerstandorten.

Der Schutzbedarf ist „normal“.

Betreibermodell

Modulare Struktur für Planung, Aufbau (i. S. Beschaffung Systemtechnik) und Betrieb mit umfänglichem Eigenbetrieb.

Aufbau/Beschaffung

Die Verträge für zusätzlich angemietete Mietleitungen laufen Ende 2014 aus.

Sachstand – Planung

Ab 2014 ist der Ausbau des Backbone-Netzes mit optischer Übertragungstechnik mit bis 10 GBit/s einschl. redundanter breitbandiger Übergänge zum DWD-Backbone geplant.

3.9 Auswärtiges Amt

Sachstand: IST-Situation

Leistungsumfang

Das weltumspannende VPN (Virtual Private Network) des Auswärtigen Amtes (AA) dient der internen Daten- und Sprachkommunikation zwischen der Zentrale in Berlin / Bonn und den Auslandsvertretungen der Bundesrepublik Deutschland. Das VPN des AA ist derzeit an den IVBB und zukünftig an NdB angebunden. Gut 12.000 Teilnehmer an ca. 230 Standorten nutzen dieses Übertragungsnetz rund um die Uhr, um die diplomatischen und konsularischen Aufgaben zu erfüllen. An Krisenstandorten oder Standorten mit schlechter örtlicher IT-Infrastruktur wird das Netz des AA auch durch Mitarbeiter anderer Ressorts mitgenutzt.

Durch den konsequenten Einsatz BSI-zertifizierter IP-Verschlüsselung (SINA-Technologie) ist das Netz zur Übertragung von bis zu VS-NfD klassifizierten Informationen zugelassen. Schnittstellen zu externen Netzen werden ausschließlich über BSI-zertifizierte Firewalls geführt. Die terrestrischen Übertragungswege haben im Mittel eine Bandbreite von 2 MBit/s. Ca. 30 Prozent der Standorte nutzen satellitengestützte Übertragungswege mit einer durchschnittlichen Bandbreite von 512 kBit/s. Um eine hohe Stabilität des Netzverbundes zu erreichen, wird als Routingprotokoll BGP-4 eingesetzt. Die hohe Verfügbarkeit der Verbindungswege ist im Rahmen eines Dienstleistungsvertrages geregelt, der u.a. eine aktive Überwachung sowie einen 24x7-Support garantiert.

Durch eine redundante Auslegung der VPN-Kernkomponenten an den zentralen Standorten Berlin und Bonn sind sowohl die Ausfallsicherheit als auch die Verfügbarkeit der Übertragungswege zu den Auslandslokationen in hohem Maße garantiert. Hardwareausfälle werden durch entsprechende Supportverträge mit den Herstellern / Lieferanten kompensiert.

Betreibermodell

Der Betrieb erfolgt durch internes IT-Personal. Die Überwachung und Kontrolle des VPN erfolgt im Schichtbetrieb 24x7 von den IT-Service- und Betriebszentren in Bonn und New York. Diesen stehen ergänzend Bereitschaftsdienste für den 3rd-Level-Support zur Seite.

Sachstand-Planung

Das Netz wird fortlaufend modernisiert. Aktuell werden vorhandene VPN-Router ausgetauscht, um den gestiegenen Anforderungen nach Performance und Stabilität gerecht zu werden.

3.10 Bundesagentur für Arbeit (BA)

Leistungsfähigkeit

Die BA betreibt derzeit zwei zentrale synchrone RZ (sowie ein Test-RZ) in Nürnberg und 11 bundesweit verteilte sog. „Server-Räume", die über ein bundesweites Weitverkehrsnetz (WAN) mit ca. 150.000 PC-Arbeitsplätzen in ca. 1.900 Liegenschaften von Bund, Ländern und Kommunen für Daten- als auch für Sprach-Kommunikation angebunden sind.

Das WAN ist ein nicht-hierarchisches IP-Mietleitungsnetz, d. h. ohne ausgeprägtes Backbone-Netz.

Der Schutzbedarf ist „Normal". Das Weitverkehrsnetz ist verschlüsselt.
Über industrieübliche Sicherheitsanforderungen (wie Verfügbarkeit und Schutz von personenbezogenen Daten) hinausgehende Anforderungen gibt es derzeit nicht.

Betreibermodell

Die ressorteigenen RZ werden durch eigenes Personal betrieben (Eigenbetrieb).
IP-Mietleitungen werden durch einen ext. DL bereitgestellt (derzeit T-Systems).
Eine Änderung ist nicht geplant.

Aufbau/Beschaffung

Das IP-Mietleitungsnetz wurde 2009 in einem EU-weiten Wettbewerb an T-Systems vergeben.

Die Vertragslaufzeit ist 5 Jahre. Das Vergabevolumen beträgt ca. 40 Mio.€/a.

Änderungen sind außer einer Neuausschreibung am Ende der jeweiligen Vertragslaufzeit sind nicht geplant.

3.11 Deutsche Rentenversicherung (DRV) Bund

Leistungsfähigkeit

Die DRV Bund betreibt derzeit zwei zentrale RZ in Berlin und Würzburg, die über ein bundesweites Weitverkehrsnetz (WAN) mit ca. 25.000 PC-Arbeitsplätzen in 66 Liegenschaften von Bund und Ländern angebunden sind.
Das WAN ist ein nicht-hierarchisches IP-Mietleitungsnetz.

Der Schutzbedarf ist „Normal". Über industrieübliche Sicherheitsanforderungen (wie Verfügbarkeit und Schutz von personenbezogenen Daten) hinausgehende Anforderungen gibt es nicht.

Betreibermodell

Die ressorteigenen RZ werden durch eigenes Personal betrieben (Eigenbetrieb). Das IP-Mietleitungsnetz vom jeweiligen externen Dienstleister.
Eine Änderung ist nicht geplant.

Aufbau/Beschaffung

Das IP-Mietleitungsnetz wurde 2009 in einem EU-weiten Wettbewerb an T-Systems vergeben. Die Vertragslaufzeit ist 5 Jahre. Die turnusmäßige Neuausschreibung wird derzeit vorbereitet.

Änderungen sind außer einer Neuausschreibung am Ende der jeweiligen Vertragslaufzeit sind nicht geplant.

4. Internationale Fallbeispiele

Im internationalen Behördenumfeld wurden exemplarisch besondere Schwerpunkte und Trends der Regierungen in USA, GB, Irland und Spanien im Aufbau und Weiterentwicklung ihrer IT-Netze analysiert, um die unterschiedlichen Tendenzen aufzuzeigen.

Die Bandbreite der Betriebsstrategien reicht von dezentral organisierten IT-Netzen mit starker Marktorientierung (Bsp. GB) bis hin zu zentralisierten Strukturen, die einen höheren Eigenbetriebsanteil des Staates vorsehen (Bsp. Spanien):

- Seit 2007 wird in Großbritannien im Zuge des PSN-Programms eine landesweite Netzinfrastruktur für Behörden aufgebaut. Das Regierungsnetz wird überwiegend durch private (auch internationale) Dienstleister betrieben und ist als Verbund dieser externen IT-Netze organisiert. Das Kerntransportnetz (GCN[2]) besteht beispielsweise als „Network of Networks" überwiegend aus privatwirtschaftlich betriebenen Netzen. Der Betrieb wurde in Form eines Rahmenvertrags für mehrere Netzanbieter ausgeschrieben. Möglichkeiten zum Eigenbetrieb der Netze durch Behörden sind in Einzelfällen vorhanden.
- In Spanien liegt der Betrieb des Behördennetzwerks SARA stärker in öffentlicher Hand. Hierbei sind verschiedene nachgeordnete Behörden des Finanzministeriums mit technischen und organisatorischen Aufgaben betraut
- In den USA wird die Weiterentwicklung von IT-Netzen der Regierung weitgehend zentral gesteuert und ist mit strategischen Regierungsprogrammen zusammengeführt - wie in den Bereichen Schutz kritischer Infrastrukturen und Verwaltungsreformen. Die Zusammenarbeit mit der Wirtschaft wird durch die öffentliche Hand stark gefördert und ist z. B. durch beratende Gremien institutionalisiert.

Die eingesetzten Instrumente zur Einflussnahme und Steuerung durch die öffentliche Verwaltung sind breit gefächert: Gestaltung von Lieferverträgen z. B.

[2] Government Conveyance Network (GCN)

über Rahmenverträge oder Verpflichtungsverträge mit Leistungsstandards, Beteiligungen in ÖPP, Prüfung/Zulassung externer Unternehmen als Betreiber von Regierungsnetzen und direkte Programm- bzw. Projektsteuerung für dies bzgl. Vorhaben.

Wesentliche Ziele für die Netzentwicklung sind insb. Erhöhung von IT-Sicherheit und Reduzierung der Kosten, was vor allem durch Marktorientierung erreicht werden soll:

- Förderung des Wettbewerbs unter den Betreibern (GB)
- Einbindung von Innovationen und State-of-the-Art Technologien aus den Unternehmen der Privatwirtschaft (Irland)
- Know-how Transfer zwischen Wirtschaft und Verwaltung (USA).

Die öffentliche Hand gibt dabei entsprechende Rahmenbedingungen vor, um eine intensive Unternehmensbeteiligung und Akzeptanz bei den Behörden zur Nutzung des Serviceangebots zu fördern:

- Reduzierung der Zugangsbarrieren für Nutzer und ext. Dienstleister als Anbieter (Irland)
- Standardisierung von z. B. zentralisierten Netzdienstleistungen, (Beschaffungs-)Prozessen oder Verträgen (GB)
- Einbindung von Unternehmen in die strategischen Planungen bei der Netzentwicklung (USA).

In der Gesamtbetrachtung wird die Entwicklung von IT-Infrastrukturen i. d. R. nicht isoliert sondern als Teil von übergeordneten Maßnahmen eingeordnet und abgestimmt - beispielsweise bei der Sicherung von kritischen Infrastrukturen oder im Rahmen der Wirtschaftsförderung (z. B. Mittelstandförderung).

In der Gesamtbetrachtung dieser Fallbeispiele lässt sich kein einheitliches Vorgehen in den betrachteten Staaten ableiten.

5. Strategische Überlegungen für die IT-Netze der öffentlichen Verwaltung

5.1 Abhängigkeit der öffentlichen Hand von IT-Systemen

Nahezu alle Prozesse und Aufgaben in der öffentlichen Verwaltung und Unternehmen sind heute IT-gestützt. Nur durch den Einsatz von IT-Systemen können die vor uns liegenden Aufgaben bewältigt werden. So ist die Energiewende nur mit intelligenten Netzen zu realisieren. Intelligente Gesundheits-, Bildungs- und Verwaltungsnetze helfen die Folgen des demografischen Wandels und die Notwendigkeit zur Kosteneinsparung bei gleichzeitig steigenden Qualitätsanforderungen in den Griff zu bekommen.[3] Die Verwendung von IT-Systemen beginnt bei der täglichen Bürokommunikation, geht über das Personal- und Finanzwesen sowie zeitkritische Abstimmungen (Vorbereitung Kabinett etc.) hinaus und reicht bis hin zu sicherheitssensiblen Aufgaben wie der Anti-Terror Datei, dem Ausländerzentralregister und der Kommunikation der Nachrichtendienste. Bei zahlreichen täglichen Vorgängen gibt es zudem die gesetzliche Pflicht zur elektronischen Datenübertragung. Die Bürgerinnen und Bürger, die Wirtschaft sowie der öffentliche Sektor (und damit des Staates selbst) sind in hohem Maße von einer funktionierenden Informationstechnik und sicheren Informationsinfrastrukturen abhängig.

Netzinfrastrukturen haben für die moderne Verwaltung die Bedeutung eines "zentralen Nervensystems" für die elektronische Kommunikation. Nahezu jede in der öffentlichen Verwaltung zu erbringende Fachaufgabe benötigt mittlerweile IT-Verfahren und behördenübergreifende IT-Netze als Grundlage - sowohl innerhalb des Bundes als auch Ebenen übergreifend. Auch die elektronische Kommunikation mit Stellen außerhalb der Verwaltung wie der Wirtschaft oder dem Bürger ist von Netzinfrastrukturen abhängig. Dabei werden der öffentlichen Verwaltung über IT-Netze auch durch den Bürger oder die Wirtschaft schützenswerte Daten anvertraut. Der Staat steht in der Verantwortung, neben der Aufrechterhaltung seiner eigenen Handlungsfähigkeit auch diese ihm übergegebenen Daten angemessen zu schützen.

[3] Empfehlungen der Wirtschafts- und Wissenschaftsvertreter der AG2 für eine nationale Strategie Intelligente Netze, Nationaler IT-Gipfel 2012.

Die Bundesverwaltung steht seit August 2009 in besonderer Verantwortung. Mit Einführung des Artikels 91c GG und des IT-NetzG wurde dem Bund die Verantwortung für das Verbindungsnetz zwischen Bund und Ländern (sowie Kommunen) übertragen. Ziel ist es, mit dem Verbindungsnetz eine sichere Plattform für einen dauerhaften und sicheren bund-/ länderübergreifenden Datenaustausch zu errichten. Mit dieser Regelung hat sich die Verantwortung des Bundes für die behördliche Kommunikation erheblich erhöht. Denn nunmehr hat der Bund auch die Verantwortung für eine hoch verfügbare und sichere Kommunikation zwischen Bundesverwaltung und Landesverwaltungen insgesamt, inkl. der Kommunikation der Sicherheitsbehörden der Länder mit denen des Bundes.

5.2 Verschärfte Cybersicherheitslage

Angesichts der erheblich gestiegenen Bedeutung von Netzinfrastrukturen, sind Netze zunehmend selber Ziel (und Mittel) von Angriffen. Das betrifft grundsätzlich alle Netze, in besonderem Maße jedoch Netze in sicherheitskritischen Bereichen wie den KRITIS-Unternehmen oder der Bundesregierung. Für Regierungsnetze hat sich die Cybersicherheitslage in den letzten Jahren dramatisch verschärft.

Zu den Top 6 der aktuellen Cyber-Angriffsformen zählen nach Einschätzung des BSI[4] derzeit Bedrohungen wie:

- Distributed Denial of Service-Angriff mittels Bot-Netzen mit dem Ziel der Störung der Erreichbarkeit von Webservern oder der Funktionsfähigkeit der Netzanbindung der betroffenen Institution
- Gezieltes Hacking von Webservern mit dem Ziel der Platzierung von Schadsoftware oder zur Vorbereitung der Spionage in angeschlossenen Netzen oder Datenbanken
- Gezielte Schadsoftware-Infiltration über E-Mail (z. B. fingierte E-Mails mit vertrautem Absender) und mithilfe von Social Engineering mit dem Ziel der Übernahme der Kontrolle über den betroffenen Rechner und anschließender Spionage

[4] BSI-A-CS 001: Register aktueller Cyber-Gefährdungen und –Angriffsformen (16.01.2012)

- Mehrstufige Angriffe, bei denen z. B. zunächst zentrale Sicherheitsinfrastrukturen (wie SSL-Zertifizierungsstellen) kompromittiert werden, um dann in weiteren Schritten die eigentlichen Ziele anzugreifen
- Drive-by-Exploits[5] zur breitflächigen Infiltration von Rechnern mit Schadsoftware beim Surfen mit dem Ziel der Übernahme der Kontrolle des betroffenen Rechners
- Ungezielte Verteilung von Schadsoftware mittels SPAM oder Drive-by-Exploits mit Fokus auf Identitätsdiebstahl.

Die Verwaltung ist zudem im besonderen Maße auch politisch motivierten Angriffen (z. B. öffentlichkeitswirksame Hackerangriffe durch Hacktivisten) und der gezielten Spionage ausgesetzt. Auf Basis von dem BSI vorliegenden Erkenntnissen ist davon auszugehen, dass ausländische Staaten (Nachrichtendienste) oder Bereiche der organisierten Kriminalität versuchen, die in Regierungsnetzen übertragenen Informationen in Erfahrung zu bringen oder zu manipulieren. Es kann auch nicht ausgeschlossen werden, dass gezielt manipulierte Hardwarekomponenten, die im Auslieferungszustand nicht dokumentierte verdeckte Zusatzfunktionen beinhalten, für spätere Angriffe genutzt werden (bei Netzwerkkomponenten bspw. gezieltes Stören der Verfügbarkeit des Netzes oder Abgreifen des Datenverkehrs).

Die Verschärfung bezieht sich damit nicht nur auf die zunehmende Quantität der Angriffe sondern auch auf die zunehmende Qualität. Angriffe auf Regierungsnetze finden täglich statt und sind der Normalzustand. Die Methoden werden immer raffinierter und die Abwehr von Angriffen erfordert einen immer höheren Aufwand. Beispiele finden sich überall:

- Täglich werden neue Schwachstellen in Software oder Hardware-Komponenten entdeckt, die potentielle Angreifer ausnutzen könnten.
- Durchschnittlich alle zwei Sekunden wird ein neues Schadprogramm beziehungsweise eine neue Variante eines Schadprogrammes erstellt.

[5] Drive-By-Exploits bezeichnen die automatisierte Ausnutzung von Sicherheitslücken. Bspw. wird bei einem Drive-By-Exploit allein durch das Anschauen einer dafür präparierten Webseite (z. B. Werbebanner mit Schadcode) ohne Nutzerinteraktion verdeckt Schadsoftware auf dem PC installiert.

- Täglich werden ca. 21.000 Webseiten weltweit mit Schadprogrammen infiziert (Dazu zählen insb. auch seriöse Webseiten, die über entsprechend kompromittierte Werbebanner ungewollt Schadprogramme verteilen).
- Mit einer Einladung zu renommierten Fachkonferenzen haben Unbekannte versucht, einen Trojaner bei Firmen der Rüstungsindustrie einzuschleusen. Wer den angehängten Flyer im PDF-Format öffnete, handelte sich über eine bis dahin nicht bekannte Lücke im Acrobat-Reader Spionage-Software ein (Meldung v. Feb. 2012).
- An den Grenzen des Regierungsnetzes IVBB sind inzwischen über 95% aller E-Mails unerwünschter Spam. Regierungsnetze werden jedoch auch mit hoch entwickelten Schadprogrammen wie individualisierten und zielgerichteten Trojaner attackiert. Diese sind in der Regel für einen sehr kleinen Empfängerkreis personifizierte E-Mails mit scheinbar vertrauenswürdigem Absender und plausiblem Betreff. Aufgrund des gezielten Einsatzes in einem sehr kleinen Empfängerkreis werden die enthaltenen Schadprogramme oftmals von gängigen Virenscannern nicht erkannt.
- Einzelne Webseiten der Bundesverwaltung werden immer wieder mit sog. DDoS-Attacken angegriffen, um die entsprechenden Seiten öffentlichkeitswirksam vom Netz zu nehmen. Regierungsnetze sollen jedoch auch zunehmend durch professionell organisierte Angriffe komplett außer Gefecht gesetzt werden: das erste in der Presse diskutierte Beispiel für die neue Qualität war der Cyberangriff auf Estland im April/Mai 2007, bei dem erstmalig eine nationale Netzinfrastruktur mit einer entsprechenden Flächenwirkung und einem großen Betroffenenkreis erfolgreich angegriffen wurde.
- Der Computerwurm Stuxnet sabotiert weltweit „erfolgreich“ Steuerungssysteme in Industrieanlagen und wurde mit außerordentlich hohem Entwicklungsaufwand erstellt. Die neue Qualität von Stuxnet ist u. a., dass auch autarke IT-Netze und -Einrichtungen betroffen sind, die nicht mit dem öffentlichen Internet gekoppelt sind.

Im Ergebnis unterliegen die Netzinfrastrukturen und IT-Systeme sowohl der öffentlichen Verwaltung als auch kritische Infrastrukturen einer besonders hohen und ständig steigenden Bedrohung sowohl der Vertraulichkeit, der Integrität aber auch der Verfügbarkeit. Der Erhalt der Handlungsfähigkeit des Staates hängt entscheidend davon ab, dass die Netzinfrastrukturen und IT-Systeme der

Verwaltungen sowie kritische Infrastrukturen gegen diese Bedrohungen wirksam geschützt werden können.

5.3 Das Leitbild zur übergreifenden IT-Netzstrategie

Die Handlungsfähigkeit von Bundes- und Landesverwaltungen – vor allem auch in besonderen Lagen – hängt vom Funktionieren sicherer IT-Infrastrukturen ab. Daher ist insb. eine hohe **Verfügbarkeit** von IT-Systemen und IT-Netzen notwendige Voraussetzung dafür, arbeits- und handlungsfähig zu sein. Neben der Verfügbarkeit sind auch **Vertraulichkeit** und **Integrität** der Daten zu gewährleisten.

In Anbetracht der Abhängigkeit der Handlungsfähigkeit des Staates von IT-Systemen und -Infrastrukturen einerseits sowie der sich zunehmend verschärfenden Cyberbedrohungslage andererseits hat der Staat eine umfassende **Gesamtverantwortung** für seine sicherheitskritischen Systeme und Infrastrukturen.
Daraus ergibt sich das Leitbild für sicherheitskritische IT-Systeme des Bundes wie folgt:

„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.“

Unter Berücksichtigung der Kriterien Sicherheit, Leistungsfähigkeit und Wirtschaftlichkeit stellt dieses Leitbild sicher, dass von Planung, über den Aufbau bis zum Betrieb der IT-Systeme und -Infrastrukturen ein konsistentes Handeln möglich ist. Im Falle von ÖPP-Projekten müssen Art und Umfang dieser Kontrolle im Sinne dieses Leitbildes vertraglich geregelt werden.

5.4 Umsetzung des Leitbilds zur übergreifenden Netzstrategie

Für die IT-Netze der öffentlichen Verwaltung wird im Folgenden ein Gesamtkonzept beschrieben, das es dem Bund ermöglicht, seine IT-Systeme und

-Infrastruktur im Sinne des Leitbildes abgestimmt und zielgerichtet weiterzuentwickeln.

Dabei sind folgende Randbedingungen zu berücksichtigen:

- Die ohnehin schon komplexe Technik folgt immer kürzeren Innovationszyklen.
- Der Staat kann im Wettbewerb um die knappen Fachkräfte nur eingeschränkt mithalten.
- Für eine größtmögliche Wirtschaftlichkeit sind möglichst viele Hersteller/Anbieter wünschenswert.
- Für besonders sicherheitskritische Komponenten können nur vertrauenswürdige Hersteller eingesetzt werden.

Unter diesen Randbedingungen kann eine undifferenzierte Umsetzung des Leitbilds im Sinne von „wir machen immer alles selber“ nicht zum Erfolg führen. Dies gilt nicht nur für den öffentlichen Sektor – auch privatwirtschaftliche Unternehmen nutzen in großem Umfang die Unterstützung von auf IT-Infrastrukturen spezialisierten Unternehmen. So lagern einige Unternehmen ihre gesamte IT-Infrastruktur an externe Dienstleister aus, während andere Unternehmen selektiv Unterstützung von Experten einholen: so werden bei großen Mobilfunknetzen für initiale Planung und Aufbau neben einem Kernteam aus eigenen Mitarbeitern externe Ressourcen mit aktuellem und ggf. notwendigem speziellen Knowhow temporär ergänzt. Das eigene Kernteam verantwortet dauerhafte neben der Gesamtarchitektur insb. auch die lfd. Anpassungen (z. B. aus betrieblichen Veränderungen).

Es ist somit eine differenzierte Umsetzung des Leitbildes erforderlich. Hierfür sollten die Phasen des Lebenszyklus eines IT-Netzes unterschieden werden. Der Lebenszyklus eines IT-Netzes enthält drei Phasen: **Planung**, **Aufbau** und **Betrieb**. Die Fähigkeiten, Kompetenzen und Erfahrungen, die für die jeweiligen Phasen notwendig sind, sind unterschiedlich. Folglich sind auch die **Betreibermodelle** und die **Beschaffungsstrategien** in den drei Phasen voneinander zu unterscheiden.

In jedem Fall ist es aber notwendig, eine eigene Kernkompetenz für diesen Bereich aufzubauen und zu erhalten, um das Leitbild und die daraus abzuleiten-

den Betreibermodelle und Beschaffungsstrategien in den Bereichen Planung, Aufbau und Betrieb umsetzen zu können.

5.4.1 Umsetzung des Leitbilds: Planung von IT-Netzen

Die Planung der IT-Netze der Bundesverwaltung erfordert eine Kombination von umfangreichen Kenntnissen der öffentlichen Verwaltung sowie tiefem und aktuellem technischen Wissen.

Umfangreiche Kenntnisse der öffentlichen Verwaltung sind erforderlich, um Anforderungen von verschiedenen Nutzern korrekt einzuschätzen und die Nutzer adäquat einzubeziehen. Weiterhin muss die Netzinfrastruktur mit einem langfristigen, politisch strategischen Blick beurteilt und geplant werden – unabhängig von aktuellen, kurzlebigen Trends.

Tiefes und aktuelles technisches Wissen ist notwendig, um die im Markt verfügbaren Technologien und Ansätze bewerten zu können und die für die öffentliche Verwaltung relevanten Technologien und Ansätze auszufiltern.

Diese Kombination von Fähigkeiten erfordert zur Umsetzung des strategischen Leitbildes somit auch eine kombinierte Leistungserbringung. Die Anforderungen an die IT-Netze sollten durch eigenes Personal festgelegt werden. Auch, die Planung der IT-Netze sollte durch **eigenes Personal geleitet und gesteuert** werden, um die Kenntnisse der öffentlichen Verwaltung einzubringen und die weitreichenden strategischen Entscheidungen selbst treffen zu können. Dazu ist es notwendig, eine eigene Kernkompetenz für diesen Bereich aufzubauen und zu erhalten. Dieses eigene Personal sollte jedoch in signifikantem Maß durch **externe Experten unterstützt** werden, die das technische Fach- und Erfahrungswissen einbringen - insb. wenn eigenes Personal nicht in erforderlicher Anzahl bzw. Qualifikation vorhanden ist oder beschafft werden kann.

Auch bei einer zeitweisen Unterstützung durch externe Dienstleister muss Know-how für Planung dauerhaft in der Bundesverwaltung als eigenen Kernkompetenz vorhanden sein bzw. geschaffen werden, um so die Planungsergebnisse bewerten und z. B. die Beschaffung der Systemtechnik ggf. auch selbst durchführen zu können.

5.4.2 Umsetzung des Leitbilds: Aufbau von IT-Netzen

Der Aufbau von IT-Netzen umfasst die Verkabelung, Installation und Konfiguration der Maschinen sowie die Implementierung von entsprechenden Diensten und Prozessen. Zusätzlich sind häufig komplexe Migrationsarbeiten notwendig, um alte Infrastrukturen – für den Nutzer möglichst unbemerkt – auf die Neuen umzustellen. Diese Arbeiten erfordern spezielles Wissen und umfangreiche Erfahrungen in ähnlichen Projekten, um bestmöglich und zielgerichtet auf die typischerweise zahlreichen Probleme während des Aufbaus eines Netzes reagieren zu können.

Diese Aufbauarbeiten erfordern sehr zahlreiche, vielfältige und sich ständig z.T. erheblich weiter entwickelnde Erfahrungen. Außerdem werden sie nicht permanent benötigt (bei Etablierung eines Netzes, bei signifikantem Ausbau eines Netzes, usw.). Spezialisierte Anbieter von IT-Infrastruktur können für den Aufbau spezialisiertes Wissen etablieren und bei einer Vielzahl von Kunden immer wieder anwenden. Die Bundesverwaltung selbst wird – mangels ausreichender Anzahl von Netz-Aufbauten und mit zunehmender angestrebter Konsolidierung immer seltener – nur schwerlich eigene, vertiefte Kompetenzen und Ressourcen aufbauen können, die eine mit spezialisierten Drittanbietern auch nur annähernd vergleichbare Kompetenz erreicht.

Somit sollte der Aufbau von IT-Netzen durch **Drittanbieter** oder **in enger Zusammenarbeit mit Drittanbietern** durchgeführt werden. Diese Drittanbieter sollten dann auch die Verantwortung und damit gleichzeitig das Risiko für den Aufbau übernehmen. Über diesen Ansatz sichert man sich die volle Motivation des Drittanbieters.

Dabei ist es im Sinne des Leitbildes von höchster Wichtigkeit, dass die Kontrolle beim Auftraggeber – dem Bund – verbleibt. Dies kann einerseits nur gelingen, wenn wie in 5.4. beschrieben eine Kernkompetenz (hier zur Steuerung und Kontrolle) aufgebaut und vorhanden ist.

Andererseits ist es notwendig, nur vertrauenswürdige Drittanbieter auszuwählen. Dies wird über die Beschaffungsstrategie erreicht. Die Beschaffungsstrategie legt Bewertungskriterien fest, nach denen die Auswahl von Drittanbietern gesteuert wird.

Dabei sollen so viele Anbieter wie möglich zugelassen werden, um den Wettbewerb zwischen den Anbietern zu fördern. Gleichzeitig wird jedoch ein hoher Sicherheitsstandard durch Auswahl vertrauenswürdiger Anbieter sichergestellt. So wird z.B. für besonders sicherheitskritische Komponenten oder Dienstleistungen die Auswahl potentieller Anbieter fallweise weiter eingeschränkt.

Wesentliche weitere Forderung für die Realisierung dieser Netze ist - neben Aufbau und Betrieb der zentralen Netzknoten in eigenen Standorten – eine robuste Basisinfrastruktur für das Leitungsnetz zwischen diesen Standorten und den Nutzerliegenschaften.

Dieses kann z. B. durch Kauf der derzeit dem Bund angebotenen bundesweiten Glasfaser-/Leerrohrinfrastruktur realisiert werden, vgl. Kapitel 3.5.

5.4.3 Umsetzung des Leitbilds: Betrieb von IT-Netzen

Die Kompetenzen, die für den **Betrieb eines IT-Netzes** benötigt werden, entwickeln sich kontinuierlich weiter, da der Betrieb einen - für die IT-Welt - relativ langen Lebenszyklus hat. Aufgebaute Kompetenzen können somit für eine relativ lange Zeit genutzt werden. Damit ist es für die Bundesverwaltung beim Betrieb einfacher als bei Planung und Aufbau Kompetenzen im notwendigen Umfang aufzubauen und vorzuhalten.

Darüber hinaus hat der Betrieb von sicherheitskritischen Komponenten wie z. B. von Kryptosystemen höchsten Einfluss auf Sicherheit und Geheimschutz, denn an diesen Maschinen wird die Verschlüsselung und Entschlüsselung durchgeführt. Somit ist die besondere Kontrolle des Betriebs für die Umsetzung des Leitbilds von größter Wichtigkeit: der Betrieb dieser Kryptosysteme erfolgt bereits heute weitgehend durch bundeseigenes Personal (z. B. im Informationsverbund der Bundesverwaltung (IVBV) durch das DLZ-IT BMVBS).

Jedoch ist auch der Einsatz von entsprechend ermächtigtem Personal vom vertrauenswürdigen externen Dienstleistern nicht ausgeschlossen.

Aus den oben genannten Gründen sollte zur Umsetzung des Leitbilds der Betrieb von IT-Netzen weitgehend durch den Bund selbst (**Eigenbetrieb**) oder un-

ter Beachtung sicherheitsrelevanter Anforderungen in Zusammenarbeit mit privaten Partnern (**öffentlich-private Partnerschaften**) durchgeführt werden.

5.4.4 Umsetzung des Leitbilds: Kompentenzaufbau

Damit der Bund die Gesamtverantwortung für seine sicherheitskritischen IT-Systeme und -Infrastrukturen wahrnehmen und somit das Leitbild erfüllen kann, nimmt er wie in den vorigen Kapiteln beschrieben bei Planung, Aufbau und Betrieb jeweils unterschiedliche Rollen ein.

Um diese Rollen wahrnehmen zu können, müssen insbesondere drei Kompetenzbereiche durch die Bundesverwaltung abgedeckt sein:

- **Strategische Kompetenzen** für eine gesamtheitliche Steuerung aller Netzaktivitäten (insbesondere in der Phase Planung)
- **Technische Kompetenzen** für Konzeption (insb. In der Phase Planung), Beschaffung (insb. in der Phase Aufbau) und Problemlösung (insb. in der Phase Betrieb) von Netzen
- Die **Kompetenz als Auftraggeber** externe und interne Aufragnehmer auszuwählen und zu steuern (insb. für Planung und Aufbau, ggf. auch in Betrieb).

Die strategische Kompetenz ist notwendig, um eine gesamtheitliche Koordinierung der Netzplanungen einzelner Ressorts unter Beachtung der gesamtstrategischen Aspekte zu ermöglichen. Nur dadurch kann eine Netz-, Projekt- und Portfoliosteuerung einschließlich gesamtheitlicher Erfolgs-, Kosten- und Risikokontrolle über verschiedene Projekte und Netze hinweg durchgeführt werden.

Die technische Kompetenz ermöglicht es der Bundesverwaltung, die Konzeptionen (insb. während der Planungsphase) durchzuführen oder zumindest zu bewerten, die Beschaffung (insbesondere während der Aufbauphase) zielgerichtet zu gestalten sowie Problemlösungen (insbesondere während der Betriebsphase) herbeizuführen.

Bei der Auftraggeberkompetenz liegen die Herausforderungen sowohl in der hohen technischen Komplexität als auch in den internen Herausforderungen, als Auftraggeber zentral über mehrere Ressorts und Behörden hinweg verschiedene Auftragnehmer zu steuern.

Um externe Auftragnehmer zu steuern, ist ein umfassendes inhaltliches Verständnis der von den Auftragnehmern zu erbringenden Leistungen notwendig. Dies gilt insbesondere bei der Definition von Schnittstellen zwischen den Verantwortlichkeiten des Auftraggebers und des Auftragnehmers. Dadurch steigt gleichzeitig die Komplexität, so dass auch vermehrt Risiken entstehen, für die ein übergreifendes Risikomanagement notwendig ist. Im Sinne dieses übergreifenden Risikomanagements ist auch die Gesamtbeurteilung der eingesetzten Hersteller und Dienstleister relevant. Unterschiedliche Anbieter und Komponenten können die Leistungsfähigkeit der Gesamtnetze gegenüber einzelnen Fehlerursachen und Risiken erhöhen. Demgegenüber ist die zunehmende operative Komplexität durch eine höhere Hersteller- und Dienstleistervielfalt abzuwägen.

Art und Umfang der Kontrolle von IT-Infrastrukturen bzw. deren ggf. erforderliche Übernahme in Krisensituationen durch den Bund sind vor diesem Hintergrund zu prüfen und im Falle von Betreiberverträgen entsprechend vertraglich zu regeln.

5.5 Bisherige Aktivitäten

Die nachfolgenden Beispiele zeigen, dass i. S. einer Gesamtverantwortung insb. für sicherheitskritische IT-Systeme und -Infrastrukturen bereits heute an vielen Stellen Kompetenzen aufgebaut und modulare Strukturen eingeführt werden.

Projekt Netze des Bundes (NdB)

NdB hat das Ziel, in einer ersten Ausbaustufe die ressortübergreifenden Netze IVBB (Informationsverbund Berlin-Bonn) und BVN (Bundesverwaltungsnetz) zu konsolidieren und eine durchgängige, einheitliche, standortunabhängige (bundesweite) und an den Anforderungen der Fachaufgaben ausgerichtete Netzinfrastruktur für Sprach- und Datenkommunikation aufzubauen.
Bereits vorgesehen ist in einer nächsten Ausbaustufe die Konsolidierung der Netze der Geschäftsbereiche von BMI, BMF und BMVBS und der Folgelösung des Bund-Länder Verbindungsnetzes (Deutschland Online Infrastruktur, DOI).

Die weitere Konsolidierungen großer Weitverkehrsnetze wie das der BA, oder der DRV Bund müssen aufgrund sehr unterschiedlicher Nutzerkreise noch geprüft werden.

NdB ist – in der ersten Ausbaustufe und mit Ausnahme des KTN-Bund – bereits modular strukturiert, so dass für Planung, Aufbau und Betrieb jeweils individuelle Betreibermodelle und Beschaffungsstrategien umgesetzt werden können.

Die technische Planung wird beispielsweise mit internen und externen Ressourcen unter interner Gesamtverantwortung durchgeführt. Hierdurch erwirbt der Bund zum Einen eigene technische Kompetenzen. Zum Anderen wird durch diese Kombination der für die Planung einer solchen Infrastruktur zwingende Input von aktuellen Entwicklungen ausreichend berücksichtigt.

Der Aufbau des Netzes sollte in der Verantwortung eines externen Anbieters liegen. Dieser Drittanbieter hätte somit auch die Verantwortung und damit gleichzeitig das Risiko für den Aufbau. Über diesen Ansatz sichert man sich die volle Motivation des Drittanbieters.

Der Betrieb soll mittelfristig soweit wie möglich mit internen Ressourcen sichergestellt werden. Mit Blick auf die Schwierigkeiten bei der Fachkräftegewinnung in der öffentlichen Verwaltung werden unter Beachtung sicherheitsrelevanter Anforderungen für den Betrieb auch alternative Organisationsformen sowie die Beteiligung privater Partner erwogen. Hierdurch könnte einerseits der Fachkräftemangel kompensiert und andererseits die Erlangung technischer Kompetenzen bei den internen Ressourcen ermöglicht werden.

Im Rahmen von NdB wird gem. Konzept „IT-Steuerung Bund“ eine Auftraggeber-Auftragnehmer Struktur („IT-Nachfrage“ vs. „IT-Angebot“) innerhalb der Verwaltung etabliert. Durch diese Konstruktion schafft der Bund zentrale Kompetenzen zur Steuerung von internen und externen Auftragnehmern und erlangt dadurch Auftraggeberkompetenzen.

Das Projekt NdB ist diesbezüglich die Basis für die aufzubauenden strategischen Kompetenzen innerhalb der Bundes-, Länder-, und Kommunalverwaltungen.

Kerntransportnetz Bund

Für das für Sicherheit und Krisenfestigkeit zentrale Architekturelement „Kerntransportnetz (KTN) Bund“, das von BDBOS und NdB gemeinsam genutzt wird, gelten besondere Anforderungen an die Vertrauenswürdigkeit möglicher externer Dienstleister.

Eine strategisch wichtige Konzepterweiterung könnte sich jedoch mittelfristig durch das aktuell vorliegende Angebot für den Erwerb einer bundesweiten Leerrohrinfrastruktur für Glasfaserleitungen für Bund und Länder ergeben. Hier muss jedoch das Ergebnis der weiteren Betrachtung dieses Themas insbesondere einer Kosten-Nutzen-Analyse abgewartet werden. Dabei sind insbesondere auch Migrationskosten bestehender Infrastrukturen einzubeziehen.

5.6 Weiteres Vorgehen

Das hier dargestellte Leitbild wird im Projekt NdB - als durchgängige, standortunabhängige und an den Anforderungen der Fachaufgaben ausgerichtete gemeinsame Netzinfrastruktur – soweit wie möglich umgesetzt. Auf dem Weg zur weiteren Umsetzung dieser übergreifenden Netzstrategie sind die Planungen weiterer Behörden und Ressorts im Hinblick auf eine **Ziellandschaft** der benötigten Netze über NdB hinaus zu harmonisieren. Für die weitere Konkretisierung dieser Ziellandschaft ist zu entscheiden, wie die darüber hinausgehenden Anforderungen der Nutzer, also der Behörden und Ministerien, am besten erfüllt werden können. Daraus ergibt sich eine mittel- und langfristige Ziellandschaft für die Weiterentwicklung von NdB.

Wie hier beschrieben, sind zahlreiche Faktoren ausschlaggebend für eine übergreifende Strategie und die Gesamtverantwortung dazu. Erst wenn diese strategischen Fragen geklärt sind, können weitere Fragen zur konkreten Umsetzung beantwortet werden. Bei der Bewertung der unterschiedlichen Betreibermodelle wäre dann auch zu beleuchten, in welchem Umfang auch Personal der öffentlichen Verwaltung gebunden ist, und in welchem Umfang die jetzt anfallenden Personalvollkosten, d.h. inkl. der Personalsachkosten der Verwaltung ergänzt werden müssen.

Im Rahmen der Konkretisierung dieser Ziellandschaft muss z. B. geprüft werden, inwiefern weitere **Netz-Konsolidierungen** durch eine Neuaufstellung aller Netze der Bundesverwaltung in einer gemeinsamen Kommunikationsinfrastruktur die Ziele Sicherheit, Leistungsfähigkeit und Wirtschaftlichkeit erfüllen.

Eventuell muss auch für die Behörden der Bundesverwaltung, die eine enge Verzahnung zum Wissenschaftsnetz und zu Forschungseinrichtungen haben, eine Lösung gefunden werden, die eine verlässliche und sichere Kommunikation innerhalb der Bundesverwaltung garantiert, aber zugleich die nötigen Freiräume zur Erfüllung der wissenschaftlichen Fachaufgaben lässt. Gleiches gilt für Behörden, die zur Erfüllung ihrer hoheitlichen Aufgaben internationale Netzeinbindungen nutzen.

Für die benötigte Verfügbarkeit muss bewertet werden, inwiefern **Redundanzen** in und zwischen den Netzen und Komponenten realisiert werden, um insb. in besonderen Lagen die Funktionsfähigkeit der Verwaltung sicherzustellen.

Die derzeitigen Netzkapazitäten sind grundsätzlich so geplant, dass sie für die Laufzeit der Verträge ausreichen. Zu klären ist für den weiteren Zeitraum, wie die Netze zum jetzigen Zeitpunkt ausgelastet sind, wie sich die Anforderung an die Kapazitäten für die Neuaufstellung oder Konsolidierung verändern und welche Auswirkungen Konsolidierungen auf die Anforderungen an die bestehenden Rechenzentren (z.B. Anzahl, Struktur) haben.

Für die Umsetzung einer Netzstrategie sind laufende oder geplante Vorhaben zu berücksichtigen. Dazu gehören insb. langlaufende Verträge, die in den nächsten Jahren auslaufen und für die Nachfolgelösungen geplant werden.

Zu den konkreten Fragen gehören:

- In diesem Bericht werden Bundesnetze, das Bund-Länder-Verbindungsnetz DOI, das Netz der Deutschen Rentenversicherung und das Netz der Bundesagentur für Arbeit betrachtet. Wie groß ist der mögliche Nutzen, wenn bei Erarbeitung konkreter Umsetzungsmaßnahmen auch die von den großen Forschungseinrichtungen (Max-Planck-Gesellschaft, Fraunhofer-Gesellschaft und Helmholtz-Gesellschaft etc.) gehaltenen Netze, die vom Bund wesentlich finanziert werden, in die Betrachtung einbezogen werden?

- Wie kann eine Zusammenarbeit und mögliche Konsolidierung des Weitverkehrsnetzes von BWI-IT („HERKULES“) mit dem zukünftigen KTN-Bund ausgestaltet werden?
  Wie können weitere Weitverkehrsbedarfe der Bundesverwaltung sinnvoll gebündelt werden?
- Gibt es Synergien bei der Konsolidierung der Netze von BA und DRV Bund?
- Ist tatsächlich ein Sicherheitsgewinn bzw. ein wirtschaftlicher Nutzen durch eine Zusammenführung der bestehenden Netzlandschaften zu erwarten?
  Bei der Bewertung des wirtschaftlichen Nutzens von Netzkonsolidierungen müssen die jeweiligen Vollkosten (Investitionen, lfd. Betriebskosten sowie die Personalvollkosten einschl. Personalsachkosten) betrachtet werden.
- Soll das aktuelle Angebot, eine bundesweite Glasfaser-/Lehrrohrinfrastruktur zu erwerben, detailliert analysiert, bewertet und ggf. angenommen und diese mittelfristig zu einem bundeseigenen Folgenetz von KTN-Bund und dem BWI-IT Weitverkehrsnetz ausgebaut werden?