Alexander Wellisch
Feuerwehr Hamburg

Breitbandanwendungen
für die nichtpolizeiliche Gefahrenabwehr

Facharbeit gemäß § 21 VAP2.2-Feu NRW

Hamburg, 16.12.2019

Aufgabenstellung

Breitbandanwendungen für die nichtpolizeiliche Gefahrenabwehr

Die Bundesanstalt für den Digitalfunk der BOS (BDBOS) hat den Auftrag, die Möglichkeiten der mobilen Breitbandversorgung für die BOS sowohl im eigenen BOS Breitbandnetz als auch in Kombination mit öffentlichen Mobilfunknetzen in einem Piloten nachzuweisen. Diskutieren Sie die Notwendigkeit und Einsatzmöglichkeit von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr. Welche Anwendungen sind momentan und in Zukunft denkbar? Beleuchten Sie dabei insbesondere die Thematik Daten- und Ausfallsicherheit.

Kurzfassung

Der Zugriff auf leistungsfähige Datenverbindungen wird heute vielfach als gesellschaftliches Grundbedürfnis postuliert. Auch in der nichtpolizeiliche Gefahrenabwehr ist die Nutzung einer derartigen Infrastruktur naheliegend, gehören doch Breitbandanwendungen zum Alltag der handelnden Personen. Die Notwendigkeit, die Einsatzmöglichkeiten und die zu berücksichtigenden Sicherheitsaspekte von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr werden in dieser Facharbeit erörtert.

Der Terminus „Breitband“ ist nicht genormt, er bedarf daher einer Einordnung. Vom Statistischen Bundesamt werden Datennetze mit einer Datenübertragungsrate von mehr 256 kBit/s als Breitbandnetz betrachtet [1]. Das Digitalfunknetz der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) bietet zum Vergleich Übertragungsraten von bis zu 28,8 kBit/s [2], weshalb es den schmalbandigen Netzen zugeordnet wird. In Deutschland wurden 2017 durchschnittliche Datenübertragungsraten im Downstream von 15.300 kBit/s erreicht [3], was die komfortable Erreichbarkeit von Webseiten und Videostreaming in HD-Qualität ermöglicht.

Die Untersuchung zeigt, dass durch die zunehmende Vernetzung der Lebens- und Arbeitsumgebung Daten generiert bzw. Informationen zugänglich werden, die für eine effiziente Gefahrenabwehr essentiell sind. Mit der Vielzahl daraus resultierender Breitbandanwendungen ist die Herausforderung verknüpft, Nutzbares von Notwendigem zu trennen. Um dieser Herausforderung gewachsen zu sein, müssen sich die BOS auf eine gemeinsame Strategie verständigen.

Breitbandanwendungen werden in nichtpolizeilichen Gefahrenabwehr derzeit nur einsatzbegleitend verwendet. Wesentliche Entscheidungen werden auf Basis konventioneller Methoden (manuelle Erkundung, Sprachübermittlung von Messergebnissen etc.) getroffen. Aufgrund des geänderten Kommunikationsverhaltens der Gesellschaft und der Vielfalt neuer Möglichkeiten zur Informationsgewinnung, Stichwort „Smart City“, sind strukturgreifende Veränderungen in der nichtpolizeilichen Gefahrenabwehr zu erwarten, die künftig die einsatzkritische Nutzung von Breitbandanwendungen erforderlich machen. Nur so kann adäquat mit den gesellschaftlichen Risiken umgegangen werden, die mir der Digitalisierung verbunden sind.

Mit der Bedeutungssteigerung von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr steigen auch die damit verbundenen Sicherheitsanforderungen. Insbesondere einem resilienten Mobilfunknetz kommt hier eine wichtige Bedeutung zu, um die erforderliche Daten- und Ausfallsicherheit zu gewährleisten. Es ist von entscheidender Bedeutung, dass die Sicherheitsbelange der BOS künftig in verstärktem Maße bei der Standardisierung des Mobilfunks Berücksichtigung finden.

Die Nutzung kommerzieller Mobilfunknetze durch die BOS wird noch für mehrere Jahre erforderlich sein, um die Entwicklung und die Erprobung spezifischer Anwendungen nicht zu behindern. Vorbehalten bezüglich der Daten- und Ausfallsicherheit kommerzieller Mobilfunknetze muss mit Strategien zum Erhalt der Handlungsfähigkeit bei Ausfall der Netzinfrastruktur begegnet werden. Dem BOS-Digitalfunknetz kommt hier eine wichtige Bedeutung zu, weshalb die langfristigen Pläne, den Betrieb des TETRA-Netzes einzustellen, aus Sicht des Verfassers erst vollzogen werden können, wenn eine alternative Netzinfrastruktur zur Verfügung steht, die mindestens gleichwertige Sicherheitsstandards gewährleistet. Parallel dazu müssen die Regelungen zur Bevorrechtigung der BOS fortgeschrieben werden, um die eingeführten Systeme zur Warnung der Bevölkerung über Mobilfunk-Endgeräte nicht zu konterkarieren.

Internationale Beispiele zeigen, dass in Europa, Asien und Amerika den Sicherheitsorganisationen bereits Breitbandtechnologien zur Verfügung stehen. Auch für die Nutzung der Potentiale einer Smart City existieren Beispiele, auf die hier eingegangen wird. Den Leitstellen der BOS kommt hier eine besondere Bedeutung bei der Aufbereitung und Nutzung von Daten zu, die für eine zeitgemäße Gefahrenabwehr erschlossen werden müssen.

Entscheidend ist, dass die BOS einheitliche Strategien entwickeln und mit IT-Experten in einen intensiven Austausch treten. Hierzu müssen Plattformen geschaffen werden, die es ermöglichen, zuverlässige Breitbandanwendungen zu entwickeln und zu erproben. Beispiele hierfür gibt es bereits. Es gehört zu den bedeutenden Aufgaben der nichtpolizeilichen Gefahrenabwehr, ihre technischen, personellen und taktischen Strukturen zu überprüfen und auf die Anforderungen einer digitalen Gesellschaft auszurichten.

In dieser Arbeit wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.

Inhalt

1 Einleitung

Ausgangssituation: *„Der digitale Wandel verändert unsere Art zu leben, zu arbeiten und zu lernen fundamental und mit rasanter Geschwindigkeit“*, so die Bundesregierung in der Umsetzungsstrategie zur Gestaltung des digitalen Wandels. [4] Im November 2019 wurden auf Schloss Meseberg weitere Maßnahmen und Strategien beschlossen, um diesem gesellschaftlichen Wandel angemessen zu begegnen. Hierbei wurde auch eine Mobilfunkstrategie vereinbart, durch die eine flächendeckende Nutzung mobiler Breitbandnetze möglich werden soll. [5] Nach einem Papier des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) sind die Belange des staatlichen Mobilfunks der BOS jedoch nicht Gegenstand der Mobilfunkstrategie, da sie einer gesonderten Betrachtung bedürfen. [6] In diesem Kontext ist der Auftrag an die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) zu sehen, der in einem Konzeptpapier [2] näher erläutert wird.

Der Eignungstest hat danach zum Ziel, einen *„Erkenntnisgewinn über die Nutzbarkeit und Ausgestaltung von hybrider Breitbandinfrastruktur für die Zwecke der BOS“* zu generieren. Als hybride Breitbandinfrastruktur wird hierbei die Nutzung kommerzieller Netze für Breitbandanwendungen der BOS mit einer Erweiterung durch eine dedizierte[1] Netzinfrastruktur betrachtet. Neben der Zusammenarbeit mit Netzbetreibern und der Praktikabilität von Netzübergängen werden die technischen Möglichkeiten für eine Priorisierung im BOS Verkehr, ein einheitliches Nutzer- und Netzmanagement, die Sicherheit und Verfügbarkeit mobiler Breitbandnetze und die rechtliche Situation untersucht. [7]

Als Breitbandnetz ist hierbei eine Datenverbindung zu verstehen, die hohe Datenübertragungsraten zulässt. Die Datenübertragungsrate ist die digitale Datenmenge, die innerhalb einer Sekunde übertragen wird [Bit/s]. Der Terminus „Breitband“ bezieht sich nach Auffassung der „International Telekommunication Union“ (ITU) jedoch weder auf eine bestimmte Geschwindigkeit, noch auf einen bestimmten Dienst. [8]

Um die Anforderungen der BOS an ein Breitbandnetz zu bestimmen, ist folglich eine Prognose der erforderlichen Datenübertragungsrate grundlegend. Die folgende Tabelle zeigt zunächst, welche Datenübertragungsraten in Abhängigkeit des Mobilfunkstandards technisch möglich sind:

Tabelle 1: Maximale Datenübertragungsraten im Mobilfunk nach Standard

Standard	2G (GSM)	3G+ (HSDPA+)	4G (LTE)	5G
Rate	220 kBit/s	42.000 kBit/s	300.000 kBit/s	10.000.000 kBit/s

(Quelle [9], eigene Darstellung)

Bei der Bemessung von Breitbandnetzen für eine Nutzung durch BOS muss berücksichtigt werden, dass es zu einer gebündelten Verwendung von Anwendungen kom-

[1] Als „dediziert“ wird in diesem Zusammenhang eine Netzinfrastruktur betrachtet, die sich unter Kontrolle von Bund / Ländern befindet und nicht mit anderen Nutzern geteilt wird.

men kann, die in Echtzeit übertragen werden müssen (z.B. Videostreaming aus mehreren Einsatzabschnitten). Zur Orientierung sind in der folgenden Tabelle die für eine unterbrechungsfreie Nutzung einzelner Anwendungen erforderlichen Datenübertragungsraten aufgeführt:

Tabelle 2: Datenübertragungsraten nach Anwendung (Richtwerte)

Anwendung	**erforderliche Datenübertragungsrate**
Messaging	10 kBit/s
Telefonie (VoIP)	100 kBit/s
Zugriff auf Webseiten	10.000 kBit/s
Videostreaming HD	9.000 kBit/s
Videostreaming FHD	16.000 kBit/s
Videostreaming UHD	25.000 kBit/s

(Quelle [10], eigene Darstellung)

Auch wenn nicht jede Anwendung in Tabelle 2 ein breitbandiges Transportnetz erfordert, müssen bei der Bedarfsbestimmung auch verhältnismäßig geringe Datenraten berücksichtigt werden, um eine gleichzeitige, unterbrechungsfreie Nutzung zu gewährleisten.

Zielsetzung: Mit der Facharbeit soll ein Beitrag geleistet werden, um die Herausforderungen und Chancen des digitalen Wandels für die nichtpolizeiliche Gefahrenabwehr zu erfassen. Das Ergebnis kann als Diskussionsgrundlage dienen, um die heterogene Struktur der nichtpolizeilichen Gefahrenabwehr auf eine einheitliche Digitalisierungsstrategie zu fokussieren.

Das Feld der nichtpolizeilichen Gefahrenabwehr wird hier bewusst breit ausgelegt, um das Gesamtsystem abzubilden. Die Nutzung von Breitbandanwendungen ist nach Auffassung des Verfassers in allen Feldern der nichtpolizeilichen Gefahrenabwehr denkbar, was auch von den befragten Experten bestätigt wird.

Methodik: Anhand eines explorativen Interviews mit dem Leiter der AG Breitband, einer allgemeinen Internetrecherche sowie einer strukturierten Literaturrecherche über den „Karlsruher Virtueller Katalog – KVK“ wurde die Basis für eine anschließende Literaturanalyse erarbeitet. Neben der Literaturanalyse wurden Experteninterviews durchgeführt, um qualitative Daten zu erheben. Die Durchführung der Interviews erfolgte nach Mieg und Brunner. [11] Eine Auflistung der Experten befindet sich im Anhang A.

Die Interviews wurden aufgezeichnet und nach Dresing und Pehl [12] transkribiert. Anschließend erfolgten eine systematische Aufbereitung und Auswertung der Daten. Da ein Personenbezug für diese Facharbeit keine Relevanz besitzt, werden die Daten in anonymisierter Form verwendet. Auf die Beifügung der Transkriptionen wird verzichtet, um Rückschlüsse auf die einzelnen Experten ausschließen zu können, was dem Wunsch der Gesprächspartner entspricht.

2 Notwendigkeit von Breitbandanwendungen

2.1 Vorbemerkung

„Neben der bisher üblichen Sprach- und Datenübertragung im BOS Digitalfunk erfordert die zunehmende Digitalisierung der BOS auch eine breitbandige Datennutzung. Gängig sind bereits die Abfragen von webbasierten Diensten zu Gefahrstoffdatenbanken und Rettungsdatenblättern. Die Anbindung digitaler Einsatzführungsunterstützungssysteme muss jederzeit an den Einsatzleitrechner oder Stabsführungssysteme möglich sein. Im Zuge der weiteren Realisierung einer Smart City wird die breitbandige Datennutzung weiter zunehmen. So müssen die verfügbaren relevanten Daten der Smart City gesichert an die Einsatzkräfte übermittelt werden.“ [13, S. 1-2]

So der Wortlaut einer Stellungnahme der AGBF Bayern zur Vergabe von Mobilfunkfrequenzen im Bereich 450 MHz, welche die Bundesnetzagentur eingeleitet hat. Der Fokus ist auf die digitale Zukunft gerichtet, wofür der Begriff „Smart City“ als Synonym gelten kann. „Smart City“ ist hierbei als Entwicklungskonzept zu verstehen, um technologische Entwicklungen für eine effizientere Gestaltung kommunaler Strukturen zu nutzen.

Auch die nichtpolizeiliche Gefahrenabwehr, als Teil der Kommunalstruktur, muss hier berücksichtigt werden, um nachhaltige Konzepte entwickeln zu können. Mit dem Begriff „Smart City“ ist der Begriff „Internet of Things“ (IoT) eng verknüpft. Der Begriff IoT bezeichnet die Vernetzung von Gegenständen untereinander und mit dem Internet. Das IoT stellt nach heutiger Vorstellung das Maximum an breitbandiger Datenübertragung dar und ist deshalb ein Untersuchungsschwerpunkt.

"Wir sind ein Teil dieser Gesellschaft. Wir bedienen uns der gleichen Mechanismen, derer sich die Gesellschaft auch bedient, und es wäre geradezu sträflich, zu sagen, wir springen auf diesen Zug nicht auf, mit der gebotenen Rücksicht darauf, was die Sicherheitsaspekte anbelangt." [14, 141–144]

Dieses im Rahmen eines strukturierten Interviews aufgezeichnete Zitat spiegelt das Verständnis wider, dass alle befragten Experten teilen. Angesichts der Herausforderungen, die mit dem digitalen Wandel unserer Gesellschaft verbunden sind, kann hier lediglich ein Diskurs zu Herausforderungen und Chancen von Breitbandanwendungen erfolgen.

2.2 Herausforderungen

Die Abgrenzung zwischen dem für die nichtpolizeiliche Gefahrenabwehr **Nutzbaren** und dem hierfür **Notwendigen** stellt nach Auffassung der befragten Experten die größte Herausforderung dar, die es zu betrachten gilt. Um diese Abgrenzung vornehmen zu können, müssen die Prozesse der nichtpolizeilichen Gefahrenabwehr analysiert werden. Hierbei sind nach Auffassung eines Experten [15] Technik, Team und Taktik zu betrachten. Nur wenn sich die Frage nach dem Zweck einer Breitbandanwendung mit einer Verbesserung der technischen, personellen oder taktischen Situation beantworten lässt, ist eine Weiterverfolgung der Idee zielführend.

Weitere wesentliche Herausforderungen, die im Rahmen von Experteninterviews [vgl. Anlage D] erörtert wurden, lauten wie folgt:

Tabelle 3: Herausforderungen von Breitbandanwendungen

Technik	Daten- / Ausfallsicherheit, Standards, Schatten-IT, Kapazitätsvorhersage
Team	Akzeptanz, Organisation
Taktik	Nutzbarkeit, Datenmenge, Rückfallebene

(eigene Darstellung)

Technik: Die Themen Datensicherheit und Ausfallsicherheit werden in Kapitel 4 behandelt. Der Begriff „Standards“ bezieht sich hier insbesondere auf die Übertragungswege inklusive der in Bezug auf die Datensicherheit erforderlichen Verschlüsselungen. Für den Gesamtkomplex IoT hat das Europäisches Institut für Telekommunikationsnormen (ETSI) im Juli 2019 einen Technischen Report veröffentlicht, der umfassende Regelungen zur Standardisierung der entsprechenden Technologie vorgibt. [16] Der Report zeigt Möglichkeiten auf, Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr zu vereinheitlichen, um deren Kompatibilität sicherzustellen.

Ein weiterer Aspekt ist die von einem Experten [15] genannte „Schatten-IT“. Gemeint ist hier die Nutzung von Soft- und Hardware unter Zugriff auf kommerzielle Netzinfrastrukturen, die nicht die Sicherheitsstandards aufweisen, die an behördliche Informations- und Kommunikationsnetze zu stellen sind (siehe Kapitel 4). Dadurch werden die hohen Sicherheitsanforderungen des BOS-Digitalfunknetzes negiert und unterlaufen.

In Abschnitt 5.3 der Feuerwehr-Dienstvorschrift / Dienstvorschrift 800 (FwDV/DV 800) [17] ist festgelegt, dass die Mitbenutzung fremder Informations- und Kommunikationsnetze nur zulässig ist, wenn keine eigenen Netze zur Verfügung stehen. Als Kommunikation wird allgemein eine Verständigung mithilfe von Sprache und Zeichen verstanden. [18] Hierfür besteht eine leistungsfähige staatliche Infrastruktur in Form des BOS-Digitalfunknetzes. Da gegenwärtig kein dediziertes Netz zur Übertragung von kapazitätsintensiven, nichtsprachlichen Informationen (Video-Streaming etc.) existiert, ist hierfür die Nutzung kommerzieller Netzinfrastrukturen vertretbar. Nach Abschnitt 5.3 FwDV / DV 800 sind dabei Einschränkungen, wie z.B. Datenschutz, Geheimhaltung, Verfügbarkeit, zu berücksichtigen.

Die Einführung eines BOS-Breitbandnetzes wird nach Expertenmeinung [19] u.a. dadurch erschwert, dass eine Kapazitätsvorhersage bislang nicht gelungen ist. Um die Voraussetzungen für eine verlässliche Kapazitätsvorhersage zu schaffen, müssen die Einheiten der BOS zunächst eine umfassende Prozessanalyse durchführen.

Team: *„Aktuell beobachten wir eine Verschiebung von den weniger digitalen Gruppen hin zu denen mit einem hohen Digitalisierungsgrad.“* [20, S. 37] Dennoch ist die Akzeptanz, Breitbandanwendungen im Rahmen der nichtpolizeilichen Gefahrenabwehr zu nutzen, aus Expertensicht eine Herausforderung. Die fehlende Akzeptanz wird darauf zurückgeführt, dass in der Gefahrenabwehr höchste Anforderungen an die eingesetzte Technik gestellt werden. Insbesondere die Ausfallsicherheit technischer Einrichtungen steht hier im Vordergrund (siehe Kapitel 4.3). Weitere Aspekte sind die Handhabbarkeit und die erforderliche Einfachheit in der Bedienung.

Eine durchgängige Organisation der Nutzung von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr ist derzeit nicht gegeben. Die FwDV / DV 800 deckt nur wenige Teile einer entsprechenden Organisationsstruktur ab. Wie in Kapitel 0 an Beispielen dargelegt wird, existieren bundesweit Insellösungen, die nicht auf Kompatibilität ausgelegt sind, was eine organisationsübergreifende Zusammenarbeit erschwert oder verhindert.

Taktik: Als Taktik wird ein aufgrund von Überlegungen im Hinblick auf Zweckmäßigkeit und Erfolg festgelegtes Vorgehen betrachtet. [21] Subsumiert man die Begriffe „Kommunikation“ und „Informationsübertragung“ unter dem Begriff „Fernmeldung“, geht es in diesem Kontext um eine Fernmeldetaktik. Diesem Begriff werden bei den BOS Funkrufnamenpläne, Meldebögen, Fernmeldeskizzen u.ä. zugeordnet. [22] Breitbandanwendungen lassen sich hier nicht einordnen.

Nach einer Expertenmeinung [23] stellt die Sicherstellung der Nutzbarkeit von Breitbandanwendungen in der Gefahrenabwehr eine Herausforderung dar. Die im privaten Sektor verbreiteten Anwendungen sind in Bezug auf der Bedienbarkeit nicht für widrige Umgebungsbedingungen, die im Rahmen der Gefahrenabwehr erwartet werden müssen, ausgelegt. Je nach Umfeld des Anwenders (Gefahrenbereich, Führungsstelle etc.) und der damit verbundenen Bekleidung, werden die Nutzungsmöglichkeiten verbreiteter Bedienoberflächen eingeschränkt. Gleichzeitig können die verbreiteten Endgeräte nicht uneingeschränkt im Rahmen der Gefahrenabwehr genutzt werden (Robustheit, Sicherheit, Bedienbarkeit), was die Auswahl Endgeräten einschränkt und ggf. Neuentwicklungen erforderlich macht.

Die Datenmenge, die bei der Nutzung von Breitbandanwendungen (Sensordaten, Videosequenzen etc.) generiert wird, ist nach Auffassung eines Experten [15] eine Herausforderung, der vorrangig zu begegnen ist. Werden Breitbandanwendungen als Führungsmittel zur Informationsgewinnung genutzt, müssen die Daten auch in der gebotenen Zeit verwertbar sein. Die übliche Führungsstruktur in der nichtpolizeilichen Gefahrenabwehr bietet gegenwärtig kein Potential für eine umfangreiche Datenaufbereitung und die Erstellung von Entscheidungsvorlagen. Die Einrichtung von Lagezentren für die nichtpolizeiliche Gefahrenabwehr und die Bildung vernetzter Leitstellen von Feuerwehr, Polizei und Rettungsdienst kann hier Abhilfe schaffen, wenngleich eine vollständige Zusammenlegung keine Vorteile erwarten lässt [24].

Der Beirat des Deutschen Städtetages und die AGBF-Bund haben sich mit der strategischen Ausrichtung der Leitstellen für die kommunale Gefahrenabwehr der Zukunft befasst. Hierbei wurde die Notwendigkeit erkannt, Prozessschritte anzupassen. Insbesondere der „Gewinnung von Daten und Informationen“, der „Verarbeitung von Informationen“ und der „Informationsweitergabe“ kommt eine besondere Bedeutung zu. [25] Der Fachausschuss Leitstellen und Digitalisierung des Deutschen Feuerwehrverbandes und der Arbeitsgemeinschaft der Leiter der Berufsfeuerwehren AGBF-Bund im Deutschen Städtetag schreibt das Dokument aus dem Jahr 2017 derzeit fort. [26]

Auf Ebene der Länder sind entsprechende Bestrebungen in NRW zu verzeichnen. Dort wird derzeit das Projekt „Vernetzung von Informationen zur Darstellung der Landeslage – VIDaL“ verfolgt. Im Mittelpunkt steht eine Lageplattform zum Austausch von

Informationen zwischen Leitstellen und Stäben. [27] In Hamburg werden die Möglichkeiten eines kontinuierlichen Informationsmanagements im Rahmen des Projektes „Erneuerung Leitstellen Feuerwehr und Polizei- PERLE“ fokussiert, wobei das Dokument der AGBF als Grundlage dient. [28]

Aufgrund der Notwendigkeit, beim Einsatz von Breitbandanwendungen auf kommerzielle Mobilfunknetze zurückzugreifen, wird von den befragten Experten zunächst von einer eingeschränkten Ausfallsicherheit ausgegangen. Nach Expertenmeinung [19, 23, 26] sind daher spezifische Rückfallebenen als Notwendigkeit zu betrachten, um die Handlungsfähigkeit der nichtpolizeilichen Gefahrenabwehr zu gewährleisten. Dies stellt eine Herausforderung dar, da der Einsatz von Breitbandanwendungen dazu verleitet, bisherige Möglichkeiten zur Informationsgewinnung etc. als veraltet zu bewerten und im Rahmen von Aus- und Fortbildungen zu vernachlässigen.

2.3 Chancen

Folgende Chancen des Einsatzes von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr wurden von den befragten Experten erkannt [vgl. Anlage D]:

Tabelle 4: Chancen von Breitbandanwendungen

Technik	Effizienzsteigerung, Dateneinsparung
Team	Effizienzsteigerung, Arbeitssicherheit
Taktik	Fernaufklärung, Einsatzdokumentation, Bevölkerungsschutz

(eigene Darstellung)

Technik: Taktische Einheiten bestehen nach FwDV 3 [29] aus der Mannschaft und den Einsatzmitteln, also Team und Technik. Dementsprechend ist die von Experten [15, 19, 23, 26] erkannte Chance der Effizienzsteigerung für Team und Technik relevant. Eine Effizienzsteigerung in Bezug auf die Technik ist hier insbesondere im Bereich der Fahrzeugtechnik zu erwarten. Beispielsweise ist für die Bedienung und Steuerung der Komponenten eines Löschfahrzeuges eine Person an das Fahrzeug gebunden. Der Maschinist kann seinen Standort bestenfalls kurzfristig verlassen. Betrachtet man die Tätigkeiten eines Maschinisten über den Einsatzverlauf hinweg, wird deutlich, dass er, nachdem die erforderlichen Aggregate in Betrieb genommen und die notwendigen Einsatzgeräte herausgegeben wurden, lediglich für den Eingriff bei Situationsänderungen (Druckabfall, Ausleuchtungskorrektur etc.) bereitsteht. Durch den Einsatz digitaler Anwendungen wäre es möglich, die Maschinistenaufgaben zu bündeln und von zentraler Stelle aus vorzunehmen. Das freigesetzte Personal könnte für Aufgaben herangezogen werden, die zwingend von Menschenhand erledigt werden müssen.

Die Chance einer Dateneinsparung [15, 23] mag zunächst als Widerspruch zu der in Kapitel 2.2 benannte Herausforderung der Datenmenge gesehen werden. Er bezieht sich allerdings nicht auf die im Rahmen des Einsatzes gewonnenen Daten, sondern auf die Möglichkeit, über Breitbandnetze auf zentrale Datenpools (Cloud) zurückzugreifen, anstatt große Datenmengen auf lokalen Computern vorzuhalten. Das sogenannte Cloud-Computing ermöglicht es zudem, die Datenaktualität zu gewährleisten.

Team: Die nichtpolizeiliche Gefahrenabwehr wird, trotz digitaler Gesellschaft, in weiten Teilen ein Handwerk bleiben. Die Arbeitseffizienz der Einsatzkräfte kann durch Breitbandanwendungen jedoch gesteigert werden, indem beispielsweise Objektdaten oder neue Erkundungsergebnisse über Datenbrillen o.ä. „vor Augen geführt werden“, um die Orientierung innerhalb eines Gebäudes zu erleichtern oder zwischenzeitlich erkundete Standortdaten von vermissten Personen zu übermitteln.

Durch den Einsatz von „Augmented Reality“ (AR) ist neben einer Effizienzsteigerung auch eine Steigerung der Arbeitssicherheit zu erwarten. So können objektspezifische Gefahren, die in Objektplänen hinterlegt sind, angezeigt oder durch Sensorelemente gewonnene Daten in Warnhinweise umgesetzt werden. Sensorelemente, die beispielsweise in die Einsatzkleidung der Trupps integriert sind, können einsatzrelevante Werte erfassen und für die weitere Einsatzplanung genutzt werden. Dadurch können Risiken besser abgeschätzt und sichere Einsatzoptionen aufgezeigt werden.

Taktik: Der Einsatz von Drohnen im Luftraum ist im privaten wie im kommerziellen Sektor inzwischen weit verbreitet, insbesondere zur Erstellung von Luftaufnahmen. Auch auf Seiten der nichtpolizeilichen Gefahrenabwehr haben sich zwischenzeitlich Einheiten etabliert, die zur Luftaufklärung an Einsatzstellen herangezogen werden können. [30] Beim Brand der Kathedrale Notre-Dame de Paris am 15. und 16. April 2019 konnte durch den Einsatz von Drohnen die Lage zügig erfasst werden, um rechtzeitig Maßnahmen zur Verhinderung einer vollständigen Zerstörung des Bauwerks zu ergreifen. [31] Diese Form der Luftaufklärung wird von den befragten Experten [15, 23, 26] als Chance gesehen, Einsatzlagen zeitgerecht zu erfassen, ohne viel Personal zu binden und zu gefährden.

Durch die Abwicklung von Einsätzen mithilfe vernetzter Geräte, die über breitbandige Datenanbindungen mit zentralen Dokumentationssystemen in Verbindung stehen, eröffnet sich nach Ansicht von Experten [15, 23] die Chance einer weitestgehend lückenlosen Einsatzdokumentation. Hierdurch kann den Dokumentationspflichten nachgekommen und eine Basis für eine fundierte Einsatzauswertung geschaffen werden. Durch eine Auswertung dieser Daten können Optimierungsmöglichkeiten in der Einsatzabwicklung verdeutlicht und eine stetige Verbesserung der nichtpolizeilichen Gefahrenabwehr erreicht werden. Auch für ein „Critical Incident Reporting System (CIRS) würde dadurch eine leistungsfähige Datenbasis generiert.

Die Bevölkerung kann heute über zahlreiche Wege zu Schadenslagen informiert werden. Trotz der Verbreitung von Anwendungen wie KATWARN und NINA, ist es bislang jedoch nicht sichergestellt, die Zivilbevölkerung örtlich präzise und zeitlich angemessen zu erreichen. Durch spezifische Breitbandanwendungen werden nach Expertenansicht [19, 23, 26] Chancen eröffnet, den Bevölkerungsschutz zu verbessern. Denkbar sind in diesem Zusammenhang Prognosen auf Grundlage von IoT-Daten und dem Einsatz von „Künstlicher Intelligenz“ (KI).

2.4 Schlussfolgerung

„Wenn Daten nicht mehr länger in Verwaltungssilos schlummern, können sie untereinander verknüpft und für datenbasierte Entscheidungen verwendet werden. Vor allem bei Katastrophenfällen ist es unabdingbar, dass die Entscheidungen aufgrund von verfügbaren Echtzeit-Daten getroffen werden“. [32, S. 182]

Aus Sicht des Verfassers wird nicht nur in Katastrophenfällen, sondern auch im alltäglichen Einsatz der Vorteil einer durchdringenden Datennutzung deutlich. Wie die Experteninterviews belegen, steht den Herausforderungen, die mit der Nutzung von Breitbandanwendungen verbunden sind, eine breite Palette an Chancen gegenüber, die den erforderlichen Aufwand rechtfertigen.

Da die Entwicklung der für die nichtpolizeiliche Gefahrenabwehr erforderlichen Instrumente auf unterschiedlichen Ebenen diskutiert und praktiziert wird, ist derzeit eine effiziente und für das gesamte Anwenderfeld zielführende Lösung nicht zu erwarten. Aus Sicht des Verfassers sollte daher BOS-übergreifend in folgenden Schritten agiert werden, die von Seiten der vfdb bereits 2017 aufgezeigt worden sind: [33]

- Bedarf und Stand der Technik definieren
  Marketing für den Mehrwehrt – Sicherheit, Schnelligkeit, Präzision – und Wirtschaftlichkeit betreiben
- Wissenstransfer sicherstellen
  Anwender, Entwickler, Produzenten und Forscher zusammenführen
- Standards definieren
- (Teil-)Refinanzierung durch Konversion (vgl. Internet)
- Forschung forcieren – neue Themen generieren
- IT-Strategie „Brandschutz“ entwickeln

Darüber hinaus muss aus Sicht des Verfassers eine „Fernmeldetaktik des digitalen Zeitalters“ entwickelt werden, um die weitestgehende Einheitlichkeit in der nichtpolizeilichen Gefahrenabwehr und der damit verbundenen Möglichkeit eines organisationsübergreifenden Einsatzes auch zukünftig gewährleisten zu können. Kommunikation und Informationsaustausch bilden hierfür die Basis, in der Zukunft stärker als in der Gegenwart.

3 Einsatzmöglichkeiten von Breitbandanwendungen

3.1 Vorbemerkung

Gegenwärtig kann das behördliche Digitalfunknetz (TETRA) lediglich für Sprach- und schmalbandige Datendienste genutzt werden. [2] Die Auswertung der Experteninterviews verdeutlicht, dass dennoch zahlreiche Breitbandanwendungen, wie Videostreaming, Patientendatenübertragung und Übertragung von Echtzeit-Lagekarten, Eingang in die nichtpolizeiliche Gefahrenabwehr gefunden haben.

Für die dieser Anwendungen werden kommerzielle Mobilfunknetze genutzt, die nicht für die Übermittlung einsatzkritischer Informationen ausgelegt sind. Als einsatzkritisch wird eine Information angesehen, deren Nicht- oder Fehlübertragung zu einer Gefährdung von Menschen, erheblichen Sachwerten oder der öffentlichen Sicherheit und Ordnung führt.

Daraus leitet sich die im Rahmen der Experteninterviews gestellte Frage ab, ob jede Kommunikation als einsatzkritisch betrachtet werden muss (vgl. Anlagen B und C). Keiner der befragten Experten sah hier eine Möglichkeit zur klaren Differenzierung zwischen „einsatzkritischer“ und „nicht einsatzkritischer“ Kommunikation, zumal eine Einschätzung in der Retrospektive unterschiedlich bewertet werden kann. Vielmehr wurde von den Experten konstatiert, dass neben der Kommunikation auch Meldungen von Sensoren einsatzkritisch sein können, die über gesicherte Datennetze übermittelt werden müssen.

Die Auswertung der der erhobenen Daten erfolgt nach Anwendungsgebiet der jeweiligen Breitbandanwendung. Die in Tabelle 5 benannten Anwendungsgebiete, wurden aus [16] entnommen:

Tabelle 5: Anwendungsgebiete von Breitbandanwendungen

Anwendungsgebiete	**Handelnde**	**Kommunikation**
Emergency Calling (EC)	Bevölkerung BOS	Zweiwegkommunikation *Bevölkerung-BOS-Bevölkerung*
Mission Critical Communications (MCC)	BOS	Gruppenkommunikation *Einsatzkraft-Einsatzkraft*
Public Warning System (PWS)	BOS Bevölkerung	Einwegkommunikation *BOS-Bevölkerung*
Automated Emergency Response (AER)	IoT-Geräte Bevölkerung BOS	Einwegkommunikation *BOS - IoT-Gerät* *IoT-Gerät - BOS* *IoT-Gerät - Bevölkerung*

(eigene Darstellung)

Die Auswertung der Experteninterviews folgt diesem Muster, wobei neben „Mission Critical Communications“ (MCC) auch „Mission Critical Data“ (MCD) unterschieden werden. Die in den 3GPP-Releases 14 und 15 definierte und gleichlautende Kategorie berücksichtigt die Übertragung von Nicht-Echtzeit-Daten für BOS-Nutzer. Die Übertragung von Echtzeitdaten wird hingegen in der Kategorie „Mission Critical Video“ geregelt. [34] Im Rahmen dieser Facharbeit wird diese Differenzierung nicht übernommen,

da beim gegenwärtigen Entwicklungsstand von BOS-spezifischen Breitbandanwendungen eine Unterscheidung als nicht vertretbar erscheint.

3.2 Gegenwärtige Einsatzmöglichkeiten

In der folgenden Tabelle sind die im Rahmen der Experteninterviews (vgl. Anlage D) und der Literaturanalyse erhobenen Daten nach den zuvor beschriebenen Anwendungsgebieten eingeordnet:

Tabelle 6: Gegenwärtige Einsatzmöglichkeiten von Breitbandanwendungen

EC	Alarmierung, Notruf-App
MCC	Echtzeit-Lagekarte, Videostreaming, Telemedizin
MCD	Datenaustausch, Datenbankzugriff, Robotersteuerung (lokal)
PWS	Messenger-Dienste, Warn-Apps
AER	eCall

(eigene Darstellung)

Emergency Calling (EC): Die Alarmierung von Einheiten der nichtpolizeilichen Gefahrenabwehr erfolgt weitestgehend durch digitale Meldeempfänger (DME) über schmalbandige Dienste. Sollen weitergehende Informationen, wie z.B. Geodaten übermittelt werden, stehen hierfür Anwendungen zur Verfügung, die über Mobilfunknetze auf das Internet zugreifen. Bei der Feuerwehr Hamburg wird ein derartiges System beispielsweise als zweiter Alarmierungsweg genutzt. [35]

Eine weitere Anwendung, die es ermöglicht, unter Nutzung mobiler Breitbandnetze Informationen zu übertragen, ist die sogenannte Notruf-App. Die vom Bundesministerium für Wirtschaft und Energie geförderte Applikation dient der Umsetzung der sogenannten Universaldienstrichtlinie[2], die den Zugang behinderter Endnutzer zu Notrufdiensten sicherstellen soll. Die Notruf-App ermöglicht es, personenbezogene Daten (Behinderungen, Grunderkrankungen etc.) an die notrufannehmende Stelle zu übermitteln. [36]

Mission Critical Communication (MCC): Nach Auffassung der befragten Experten [15, 23, 30] sind Anwendungen, die eine hohe Übertragungsrate erfordern (GIS-Datennutzung, Videoübertragungen etc.), heute generell möglich, sofern auf kommerzielle Breitbandnetze zurückgegriffen wird. Die Feuerwehr Hamburg hat hierzu ihre Einsatzfahrzeuge mit Kopfstellenroutern ausgestattet, die auf ein kommerzielles Mobilfunknetz zugreifen, um an Einsatzstellen ein WLAN auszubreiten. Hierdurch wird ein breitbandiger Zugriff auf sämtliche Büro- bzw. Fachanwendungen sowie das Internet ermöglicht. Zudem können Videokonferenzen durchgeführt werden, um Abstimmungen zwischen den Entscheidungsdistanzen (Stab, Technische Einsatzleitungen, Einsatzabschnittsleitungen) vorzunehmen. [37]

[2] Richtlinie 2002/22/EG geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009

Das lokale Funknetz ermöglicht es, allen Behörden der FHH an der Einsatzstelle auf deren Intranet und das Internet zuzugreifen, wodurch die fachübergreifende Zusammenarbeit ideal gestaltet werden kann. Der IT-Dienstleister der FHH, eine Anstalt des öffentlichen Rechts, bietet zudem einen behördlichen Messenger-Dienst an, der eine datenschutzkonforme Nutzung ermöglicht.

Über das Einsatzstellen-WLAN wird auch die Kommunikation zwischen den einzelnen Führungsmitteln sichergestellt. Über eine Führungsunterstützungsanwendung kann in Echtzeit kommuniziert werden, um ein umfassendes Lagebild zu gewährleisten.

Experten [15, 23, 26] weisen darauf hin, dass im Bereich der medizinischen Rettung bundesweit über die Einführung von Telenotarzt-Modellen diskutiert wird. Die Landesregierung in Nordrhein-Westfalen verfolgt das Ziel, landesweit ein derartiges Modell einzuführen. Als Vorbild dient das bereits eingeführte Aachener Telenotarzt-Modell, bei dem ein Notarzt von der Leitstelle aus die Rettungsmittelbesatzungen unterstützt. [38]

Mission Critical Data (MCD): Eine Voraussetzung für ein Telenotarzt-Modell ist die Übertragung von Patientendaten. Auch beim Einsatz von Notärzten an Einsatzstellen ist die entsprechende Datenübertragung mittlerweile ein wichtiger Baustein, um die Patientenversorgung zu optimieren. In Hamburg wird der Informationsaustausch zwischen den vor Ort bzw. auf Anfahrt zum Krankenhaus befindlichen Rettungsmitteln und den Notaufnahmen flächendeckend praktiziert. Hierbei werden die Versicherungsdaten des Patienten, die von Medizingeräten erhobenen Daten (Elektrokardiogramm, Beatmungsstatus etc.) sowie, nach Bedarf, Fotoaufnahmen übertragen. In der Rettungsleitstelle und den Zielkliniken werden die Daten aus den anfahrenden Rettungsmitteln auf Bildschirmen angezeigt und entsprechend verarbeitet. [39]

Neben dem Zugriff auf spezifische Datenbanken, wie beispielsweise Gefahrstoffdatenbanken, ist der einsatzbezogene Zugriff auf das Internet von zunehmender Bedeutung zur Informationsgewinnung. Nach einer Studie im Auftrag des Presse- und Informationsamtes der Bundesregierung spielen digitale Medien bei der Informationsbeschaffung der Generation Y, die zwischenzeitlich auch in Führungsfunktionen der nichtpolizeilichen Gefahrenabwehr präsent ist, für 93 % der Befragten eine dominierende Rolle. [40, S. 45] Ein vor äußeren Zugriffen gesicherter Internetzugang wird an den Einsatzstellen der Feuerwehr Hamburg beispielsweise über das zuvor beschriebene WLAN gewährleistet.

Der Einsatz von ferngesteuerten Einsatzgeräten, wie beispielsweise dem sogenannten Löschroboter LUF 60, der bei den Feuerwehren Stuttgart und Hamburg genutzt wird, oder dem Manipulator „Brokk 120 D“, der 2019 vom Kampfmittelräumdienst der Feuerwehr Hamburg in Betrieb genommen wurde, ist bei Einheiten der nichtpolizeilichen Gefahrenabwehr bereits verbreitet. Diese Einsatzgeräte werden allerdings über Funkfernsteuerungen (Remote Control) bedient, die nicht auf Mobilfunknetze zugreifen, weshalb sie nicht als Breitbandanwendungen betrachtet werden können. Allerdings existieren auf dem Markt ferngesteuerte Einsatzgeräte, die über Tablets oder Smartphones gesteuert werden können, wie der sogenannte Löschroboter TC800-FF,

der von der Pariser Feuerwehr (BSPP) beim Brand von Notre-Dame de Paris eingesetzt worden ist. [31] Die Voraussetzung für den Einsatz dieser Geräte ist der Zugriff auf breitbandige Mobilfunknetze.

Public Warning System (PWS): Kommerzielle Nachrichtendienste werden seit mehreren Jahren von Einheiten der nichtpolizeilichen Gefahrenabwehr genutzt, um Warnhinweise zu geben. Beispielweise wurde beim Elbehochwasser 2013 der Kurznachrichtendienst Twitter verwendet, um der vom Wasser eingeschlossenen Bevölkerung Hilfe anzubieten und auf bevorstehende Evakuierungsmaßnahmen hinzuweisen. [32, S. 56] Die Nutzung von kommerziellen Kurznachrichtendiensten erfolgt hierbei i.d.R. parallel zu Warn- und Informationssystemen wie NINA oder KATWARN.

Für die Ligurische See wurde, unterstützt vom französischen Staat, zwischen 2009 und 2011 ein Frühwarnsystem entwickelt (RATCOM), das auf Überflutungsgefahren, beispielsweise infolge eines Tsunami, hinweisen soll. [16, S. 42] Das Warnsystem basiert auf einer Vernetzung über breitbandige Datendienste.

Automated Emergency Response (AER): Laut einer EU-Verordnung[3] müssen seit 31.03.2018 neu genehmigte Fahrzeugtypen über ein automatisches Notrufsystem (e-Call) verfügen. In Oberklassefahrzeugen ist diese Sicherheitseinrichtung zur automatischen Absetzung eines Notrufes bereits seit rund 15 Jahren verbreitet. Einheiten der nichtpolizeilichen Gefahrenabwehr ist es hierdurch möglich, entsprechend ausgestattete Unfallfahrzeuge präzise zu lokalisieren und die Interventionszeiten dadurch zu verkürzen. Vergleichbare Konzepte existieren auch in der Russischen Föderation (ERA-GLOSNASS) und den Vereinigten Staaten von Amerika (E911).

Automatische bzw. manuell auslösbare Notrufe über eCall-Einrichtungen erfordern zwar kein Breitbandnetz, da der zu übertragende Minimaldatensatz nur 140 Byte umfasst, langfristig werden jedoch keine schmalbandigen Netze mehr zur Verfügung stehen, da im Zuge des 5G-Netzausbaus die 2G/3G-Netze sukzessive abgeschaltet werden sollen. Die Datenübertragung bzw. die Kommunikation mit der zuständigen Rettungsleitstelle wird dann über breitbandige Mobilfunknetze erfolgen.

Entsprechende Systeme existieren auch für IoT-Elemente wie Smartwatches [41]. Hier wird über Sturzsensoren eine potentielle Notsituation erkannt und an einen hinterlegten Kontakt gemeldet, wobei auch Standortdaten übermittelt werden. Vergleichbare Systeme werden auch als Hausnotrufsystem, z.B. für Senioren angeboten. Eine umfassende Untersuchung zu diesem Anwendungsbereich wurde in dem vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekt „Smart Senior“ untersucht. [42] Das Projekt umfasste u.a. die Untersuchung erweiterter Ortungssysteme, die in einer Notsituation mit dem jeweiligen Standort auch die Vitaldaten des Fahrers an eine notrufannehmende Stelle übermitteln. [32, S. 155-156] Eine durchgängige Anbindung dieser Komponenten an staatliche Rettungsleitstellen ist jedoch, im Gegensatz zu eCall-Systemen, bislang nicht gewährleistet.

[3] Verordnung (EU) 2015/758 des Europäischen Parlaments und Rates vom 29.04.2015

3.3 Zukünftige Einsatzmöglichkeiten

Der Blick in die Zukunft setzt voraus, dass eine leistungsfähige Netzinfrastruktur zur Verfügung steht, die den Sicherheitsanforderungen der BOS (siehe Kapitel 4) entspricht und eine Echtzeit-Datenübertragung ermöglicht. Auf Grundlage der Experteninterviews und den Ergebnissen der Literaturanalyse können folgende Einsatzmöglichkeiten herausgestellt werden:

Tabelle 7: Zukünftige Einsatzmöglichkeiten von Breitbandanwendungen

EC	Big Data Analytics/IoT
MCC	IT-gestützte Erkundung
MCD	Big Data Analytics, Echtzeit-Routing, Holografie/Augmented Reality, BIM-Daten, Fernmanipulation, Fernaufklärung
PWS	Drohnen
AER	Wearable Computing, Big Data Analytics/IoT

(eigene Darstellung)

Emergency Calling (EC): Das Potential von „Big Data Analytics“ zur Vorhersage von möglichen Gefahrensituationen wurde insbesondere in den Vereinigten Staaten von Amerika erkannt. [43, S. 152] „Big Data Analytics“ ist hierbei der Schlüssel, um große Datenmengen, die z.B. von IoT-Elementen generiert werden, in nutzbare Informationen für die Gefahrenabwehr zu transformieren.

Auch das Europäische Institut für Telekommunikationsnormen hat in einer aktuellen Publikation [16] auf die Chancen hingewiesen, die durch Big Data Analytics bestehen. In Bezug auf das hier thematisierte Segment (EC) wurde festgestellt, dass mehrere kommerziell verfügbare Technologien existieren, die eine automatische oder semiautomatische Notruffunktion ermöglichen. Als Beispiel wurden Brandmeldesensoren, CBRN-Sensoren, eCall-Funktionen, Notsignale von Flugzeugen und Schiffen sowie Waldbranddetektoren und Wasserstandsensoren genannt. [16, S. 41]

Die Anbindung von Brandmeldesensoren bezieht sich hierbei nicht auf Brandmeldeanlagen in Sonderbauten, sondern die Anbindung jeglicher Sensorik, die in der Lage ist, einen Gebäudebrand zu detektieren. Gegenwärtig mag dies in Anbetracht einer Vielzahl von Täuschungsalarmen durch standardisierte Brandmeldeanlagen illusorisch erscheinen, durch die Einbeziehung weiterer Gebäudedaten (Big Data Analytics) ist eine verlässliche Gefahrenmeldung jedoch durchaus denkbar. In jedem Fall ist festzustellen, dass in diesem Segment (EC) ein hohes Entwicklungspotential besteht.

Mission Critical Communication (MCC): In den vergangenen Jahren wurden mehrere nationale Forschungsprojekte durchgeführt, die zum Gegenstand hatten, einen Massenanfall von Verletzten (MANV) durch IT-Anwendungen zu unterstützen (z.B. e-Triage, SOGRO, TOXI-Triage). Folgende Ziele wurden hierbei verfolgt: [16, S. 42]

- Beschleunigte Erfassung der Situation vor Ort
- Medienbruchfreie Kommunikation für eine sichere und schnelle Einsatzführung
- Entwicklung patientennaher Diagnosemethoden inkl. Triagierungsmöglichkeit

Neben einer derartigen IT-gestützten Erkundung im Falle eines MANV ist eine Ausweitung auf den Gesamtbereich der Erkundung in der nichtpolizeilichen Gefahrenabwehr denkbar, beispielsweise durch die nonverbale Mitteilung von Erkundungsergebnissen an die übergeordneten Führungskräfte. Beispielsweise könnten Gefahrenbereiche, betroffene Personen, drohende Ereignisse etc. digital mitgeteilt und mit Gebäudedaten verknüpft werden (Geschoss, Nutzungseinheit, Raum etc.).

Auch die Kommunikation mit Objekten (IoT) wird eine mögliche, ggf. sogar notwendige, Breitbandanwendung für die nichtpolizeiliche Gefahrenabwehr sein. [15, 26] Beispielsweise werden Gebäude, in Zukunft noch stärker als in der Gegenwart, durch digitale Schließsysteme gesichert. Der bisher im Rahmen der Gefahrenabwehr praktizierte „gewaltsame Zugang“ zu einem Objekt wird hierdurch zunehmend schwerer umzusetzen sein. Durch eine „Public-Key-Infrastructure“ könnte den BOS die Möglichkeit gegeben werden, einen autorisierten und abgesicherten Gebäudezugang zu realisieren.

Mission Critical Data (MCD): „Big Data Analytics“ kann neben dem Segment „Emergency Calling“ auch im Segment „Mission Critical Data“ hilfreich sein. So können bei Großveranstaltungen Prognosen von Personenströmen genutzt werden, um die Einhaltung der Kapazitätsgrenzen von Fluchtwegen zu überwachen und die Möglichkeit zu erhalten, frühzeitig gegenzusteuern. [32] Auch Prognosen zur Wetterentwicklung oder zur Entwicklung der Verkehrssituation können zur Abwendung von Gefahren herangezogen werden. [32, 32, S. 61-62] Die BOS werden dadurch in die Lage versetzt, proaktiv zu handeln, anstatt zu reagieren.

Proaktiv zu handeln anstatt auf eine vorgefundene Situation zu reagieren ist auch bei Einsatzfahrten hilfreich. Gerade in Ballungsräumen führen hohe Verkehrsdichten, ausgelöst durch Straßensperrungen, unerwartete Ereignisse oder tageszeitabhängige Überlastungen, zu Schwierigkeiten in der Erreichung der festgelegten Eintreffzeiten. Durch die Überlagerung von Echtzeit-Verkehrsdaten, die von kommerziellen Datendiensten kontinuierlich erhoben werden, und Daten der Verkehrsbehörden ist aus Expertensicht [15, 39] ein sogenanntes „Echtzeit-Routing“ denkbar, um Fahrtrouten vorausschauend zu berechnen. Auch hierbei handelt es sich um „Big Data Analytics“.

Die Nutzung von „Holographic Augmented Reality“, also der Erweiterung der Realität durch eine Überlagerung mit digitalen Informationen, wurde von Experten als künftige Möglichkeit zur Optimierung der Ausbildung [26] und der Gefahrenabwehr [15] genannt. In Bezug auf die Gebäudebrandbekämpfung kommt hierbei BIM-Daten eine besondere Bedeutung zu. [44, S. 85] Auch international wird diese Breitbandanwendung als zukunftsträchtig angesehen. [43, S. 150-151]

Die Nutzung von unbemannten Land-, Luft- oder Wasserfahrzeugen ermöglicht es, Gefahrensituationen für Einsatzkräfte zu minimieren. Das BMBF fördert daher die Forschung zu Drohnen und Robotern für die Gefahrenabwehr. [45] Hierbei soll, im Gegensatz zu gegenwärtig eingesetzten Drohnen und Hilfsgeräten, ein autonomer Einsatz der Fahrzeuge möglich sein, was entsprechend breitbandige Datenanbindungen voraussetzt. Als spezifische Aufgabengebiete können hierbei die Fernaufklärung, z.B. von einer Rettungsleitstelle aus, oder die Fernmanipulation genannt werden.

Drohnen und Roboter sind hierbei als spezielle IoT-Komponenten zu betrachten, die multifunktional einsetzbar sind, z.B. zur Informationsgewinnung, zur Warnung der Bevölkerung oder für Transportaufgaben. [16, S. 40-41] Für die Seenotrettung wird derzeit untersucht, wie Flügel-Drohnen bei der Suche nach im Wasser schwimmenden Menschen eingesetzt werden können. Es wird erwartet, dass über hochentwickelte Kamerasysteme auch bei schlechten Sichtverhältnissen Menschen zuverlässig geortet werden können. [45]

Derzeit wird bei der Feuerwehr Hamburg das Projekt „Zentrales Datenmanagement“ finalisiert. Vorgesehen ist hierbei, dass das künftige Lagezentrum der Feuerwehr u.a. an folgende Daten- und Informationsquellen angebunden wird, um eine vorausschauende Gefahrenabwehr sicherstellen zu können: [39, S. 17]

- Luftmessnetz
- Verkehrssituation (Straßensperrungen, Stau) in Echtzeit
- ÖPNV-Auslastung (Hochbahn/S-Bahn/Busse)
- Aktuelle Übersicht Gefahrgüter im Hafen
- Klinikausauslastung und freie Behandlungskapazitäten in den Kliniken
- Privathaushalte (Rauchmelder, Kameras, Gebäudezugangssysteme)
- Gebäudemanagementsysteme
- Passagierlisten von Fluggesellschaften

In Bezug auf den Rettungsdienst sind im Rahmen des Projektes „Zentrales Datenmanagement“ u.a. folgende Maßnahmen geplant: [39, S. 15]

- Automatische Berechnung der Ankunftszeit und aktives Routing
- Auswahl der Zielklink nach „Matching“ und günstigster Fahrtroute
- Übertragung der GPS-Position des Patienten (Auffindeort) bei der Vorsichtung in die Stabssoftware
- Übertragung der Sichtungskategorien aus Vorsichtung und ärztl. Sichtung in die Stabssoftware
- Ausstattung der RTW mit Übertragungstechnik (Kamera, Mikrofon)

Public Warning System (PWS): Die Datenauswertung führt in Bezug auf das Segment PWS zu der Erkenntnis, dass durch den Einsatz autonomer Drohnen eine Verbesserung in Bezug auf die Bevölkerungswarnung zu erwarten ist. [16, S. 40-41] Zudem können durch die zunehmende Ausweitung des IoT weitere Potentiale für dieses Segment erschlossen werden. Denkbar ist hier die Nutzung öffentlich zugänglicher Displays oder privater IoT-Endgeräte (SmartTV, Smart Watch etc.) zur Warnung der Bevölkerung. [16, S. 79]

Automated Emergency Response (AER): Auch mit diesem Segment ist das IoT eng verknüpft. Der Terminus IoT wird hierbei in verschiedenen Zusammenhängen genannt – vom Sensor bis zur Smart City. Es existiert auch die Auffassung, dass es sich um „Internet of Everything“ handelt, werden doch auch Dinge, über „connected wearables“ mit Personen vernetzt. [43, S. 151-152]

Das Erkennen und Lokalisieren von Notfällen, die Registrierung von Lebenszeichen verletzter Personen, die Erfassung der Vitaldaten von Einsatzkräften etc. kann als

Breitbandanwendung der Zukunft für die nichtpolizeiliche Gefahrenabwehr betrachtet werden. Hierdurch können Sicherheitsstandards (security/safety) gehoben, Interventionszeiten verkürzt und die Effizienz von BOS gesteigert werden. [43, S. 151-152]

Sensoren an den Körpern und der Schutzkleidung des Einsatzpersonals können in Verbindung mit vernetzten Kameras dazu genutzt werden, permanent wichtige Informationen wie Position, Vitaldaten u.ä. zu erfassen, wodurch die Sicherheit der Einsatzkräfte und die Gesamteffizienz des Einsatzes gesteigert werden können. Die gewonnen Informationen können zudem in Echtzeit an Entscheidungsträger übermittelt werden, um die Grundlage für zeitgereichte und zielgerichtete Entscheidungen zu treffen. [43, S. 151-152]

IoT, und damit „Big Data Analytics“, repräsentiert den nächsten Schritt der Digitalisierung, in der alle physischen Objekte, Maschinen, Server, andere Endgeräte und Menschen über Kommunikationsnetzwerke miteinander verbunden sein können. Über alle privaten, öffentlichen und industriellen Bereiche hinweg wird deren Status und der Status der umliegenden Geräte erfasst und die gewonnen Daten ausgetauscht. [16, S. 14]

3.4 Schlussfolgerung

Bei der Analyse gegenwärtiger und zukünftiger Einsatzmöglichkeiten von Breitbandanwendungen wird deutlich, dass leistungsfähige Mobilfunknetze den limitierenden Faktor darstellen. Die gegenwärtigen Einsatzmöglichkeiten sind davon geprägt, dass regional unterschiedliche Mobilfunkstandards verfügbar sind, die unterschiedliche Datenübertragungsraten zulassen (siehe Tabelle 2).

Der Blick in Zukunft setzt, wie anfänglich erwähnt, ein leistungsfähiges Mobilfunknetz voraus. Die sich derzeit im Aufbau befindlichen 5G-Netze (Berlin, München, Hamburg, Frankfurt am Main und Köln) werden zumindest in Teilbereichen der Metropolen als Testfeld für die nichtpolizeiliche Gefahrenabwehr genutzt werden können. Bevor Anwendungen wie autonome Drohnen, Augmented Reality und Big Data Analytics regelhaft für die nichtpolizeiliche Gefahrenabwehr zur Verfügung gestellt werden können, muss zunächst deren Rolle geklärt werden.

Gegenwärtig wird Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr jedoch lediglich eine einsatzbegleitende Rolle zugesprochen. [14] Einsatzkritische Sachverhalte werden weiterhin mittels BOS-Digitalfunk über Sprachmeldungen kommuniziert. Bei der Notrufannahme und der Alarmierung von Einsatzkräften sowie für die Warnung der Bevölkerung erfolgt jedoch zunehmend ein Zugriff auf Breitbandanwendungen. Ein Blick auf nationale und internationale Entwicklungen auf dem Sektor der nichtpolizeilichen Gefahrenabwehr lässt erwarten, dass in Zukunft ein Wandel vom einsatzbegleitenden zum einsatzkritischen Instrument stattfindet.

Durch die zunehmende Vernetzung von Endgeräten über das Internet, nach dem US-amerikanische Telekommunikationsunternehmen CISCO werden bis 2030 weltweit 500 Milliarden Endgeräte über das Internet miteinander verbunden sein [46], ist der Übertragung von Daten auch für die Gefahrenabwehr künftig ein höherer Stellenwert

beizumessen. Aufgrund der hierbei zu erwartenden Datenmengen ist eine Nutzung des Instrumentes „Big Data Analytics“ unverzichtbar.

In der Gegenwart müssen die Voraussetzungen geschaffen werden, um auch in der Zukunft eine zeitgemäße Gefahrenabwehr ausüben zu können. Aus Sicht des Verfassers ist es daher notwendig, dass BOS, Softwareentwickler und die Industrie eine Kommunikationsebene finden, um neben der Industrie 4.0 auch die Feuerwehr 4.0 [33] zu entwickeln. Wenn es darum geht, eine „Smart City“ zu schützen, müssen auch die BOS technologisch und organisatorisch auf der Höhe der Zeit sein.

Bei allem Innovationswillen darf jedoch eine realistische Einschätzung der Gefährdungslage und der Notwendigkeit von technischen Systemen nicht ausbleiben, wie führende Wissenschaftler verdeutlichen: [47]

„Smart City“ wird häufig mit Sicherheitsversprechen verbunden. (...) Sicherheitsversprechen adressieren die vermeintliche Allgegenwärtigkeit von Bedrohungen. (...) Wenn Sicherheit und Unsicherheit als Leitmotive der Stadtentwicklung beschrieben werden können, dann ist der Smart-City-Diskurs für die Vermarktung neuer Technologien eine willkommene Rahmung und notwendige Bedingung der Durchsetzung privater sowie staatlicher Raumkontrolle.“ [48, S. 127]

4 Sicherheitsaspekte von Breitbandanwendungen

4.1 Vorbemerkung

Laut der Aufgabenstellung sollen insbesondere die Daten- und Ausfallsicherheit von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr beleuchtet werden. Hierfür ist eine Betrachtung der **Informationsinfrastruktur** erforderlich, die nach der Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI) die IT-Infrastruktur und die Telekommunikationsinfrastruktur (TK-Infrastruktur) umfasst. [49]

IT-Infrastruktur: *„IT-Infrastruktur bezeichnet alle materiellen und immateriellen Güter, die den Betrieb von (Anwendungs-) Software ermöglichen.“* [50]

TK-Infrastruktur: *„Telekommunikationsinfrastrukturen beschreiben die physischen Elemente/Bestandteile (z.B. Rohre, Kabel, Masten, Schächte), die eine raumüberbrückende Kommunikation ermöglichen.“* [51]

Da Sprache (TK) und Daten (IT) heutzutage zum größten Teil auf Basis der gleichen technischen Verfahren und die gleichen Netze übertragen werden, weist das BSI die beiden Branchen gemeinsam dem Informations- und Kommunikationssektor (IKT-Sektor) zu. [52, S. 108] Innerhalb dieser KRITIS-Branchen werden die Dienstleistungen Sprach- und Datenübertragung sowie Datenspeicherung und -verarbeitung als KRITIS-relevant (kritisch) definiert und behandelt.

Kritische Infrastruktur (KRITIS): *„Einrichtungen und Organisationen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“* [53, S. 18]

Sicherheitsanforderungen an die Informations- und Kommunikationstechnik (IuK-Technik) in der nichtpolizeilichen Gefahrenabwehr sind in der Feuerwehr-Dienstvorschrift / Dienstvorschrift 800 „Informations- und Kommunikationstechnik im Einsatz“ (FwDV / DV 800) [17] festgelegt. Darin ist der Grundsatz verankert, dass nur IuK-Technik einzusetzen ist, welche die Vertraulichkeit, die Verfügbarkeit und die Integrität von Daten im jeweils erforderlichen Maße gewährleistet.

Die genannten Schutzziele sind identisch mit der sogenannten „CIA-Triade“ (Confidentiality, Integrity, Availability) in der Informationssicherheit, folgendermaßen definiert sind:

Tabelle 8: Schutzziele der Informationssicherheit

Schutzziel	**Bedeutung**
Vertraulichkeit	Daten sind für unberechtigte Dritte nicht zugänglich
Integrität	Daten können nicht verfälscht werden
Verfügbarkeit	Daten stehen zur Verfügung, wenn sie gebraucht werden

(eigene Darstellung)

Diese Sicherheitsanforderungen werden bei der Nutzung des TETRA-Digitalfunknetzes mit den hierfür zugelassenen Endgeräten erfüllt. Insbesondere die Verfügbarkeit der Daten wird gewährleistet, da das TETRA-Digitalfunknetz, neben einer Netzabdeckung von 99 % des Bundesgebietes [54], in den wesentlichen Komponenten redundant ausgelegt und mit leistungsfähigen Ersatzstromanlagen ausgestattet ist. [55]

Da Breitbandanwendungen für die nichtpolizeiliche Gefahrenabwehr grundsätzlich mobil einsetzbar sein müssen, kommt als IKT-Infrastruktur lediglich ein Mobilfunknetz in Betracht. Feste Zugangspunkte in das kabelgebundene Breitbandnetz sind nicht praktikabel, da deren Inbetriebnahme zeitaufwändig ist und die erforderlichen Knotenpunkte nicht in Einsatzstellennähe zu erwarten sind.

Wie schon in der Kurzfassung ausgeführt, ist das TETRA-Digitalfunknetz nicht für breitbandige Datendienste ausgelegt, weshalb von den Einheiten der nichtpolizeilichen Gefahrenabwehr, die bereits Breitbandanwendungen nutzen, auf kommerzielle IKT-Infrastruktur zurückgegriffen wird. Die Nutzung der kommerziellen IKT-Infrastruktur wird auch beim aktuellen Test der AG Breitband [2] berücksichtigt, da ein dediziertes Netz alleine nicht alle Einsatzszenarien abdecken kann. [56]

Ob und wann ein dediziertes Breitbandnetz für die BOS zur Verfügung steht ist derzeit unklar. Aktuell sind die hierfür erforderlichen Frequenzen nicht zugeteilt und die BDBOS steht in Konkurrenz zu Teilen der Energiewirtschaft. [7] Die folgende Betrachtung in Bezug auf die Daten- und Ausfallsicherheit von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr ist daher auf kommerzielle IKT-Infrastrukturen fokussiert.

4.2 Datensicherheit

„Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist „Informationssicherheit“. [57, S. 61]

Das BSI hat in dem 2019 in 2. Edition erschienenen IT-Grundschutz-Kompendium [57] 47 „Elementare Gefährdungen“ aufgeführt, die von Feuer, über Wasser zu Naturkatastrophen und Sabotageakten reichen. Der Rahmen einer Facharbeit lässt es nicht zu, alle potentiellen Gefahren für die Informationssicherheit darzustellen bzw. zu diskutieren.

Die Literaturauswertung hat ergeben, dass die kommerziellen IKT-Unternehmen, wie beispielsweise die Deutsche Telekom, ausführliche Standards etabliert haben, um die Informationssicherheit für Ihre Kunden zu gewährleisten. [58] Für den Verfasser, als IKT-Laien, ist es nicht möglich, die Einzelmaßnahmen kommerzieller IKT-Unternehmen zu bewerten. Die Experteninterviews haben ergeben, dass nicht die Standards kommerzieller Unternehmen als maßgebend angesehen, sondern die vom BSI definierten Standards als geeignete Grundlage betrachtet werden. Daher wird im Weiteren ausschließlich auf BSI-Standards eingegangen.

Da der Schutzbedarf i.d.R. nicht quantifizierbar ist, beschränkt sich der IT-Grundschutz (BSI) auf qualitative Aussagen, wie in der folgenden Tabelle dargestellt:

Tabelle 9: Schutzbedarfskategorien nach IT-Grundschutz (BSI)

normal	Die Schadenauswirkungen sind begrenzt und überschaubar.
hoch	Die Schadensauswirkungen können beträchtlich sein.
sehr hoch	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

(eigene Darstellung)

Bezogen auf die nichtpolizeiliche Gefahrenabwehr wird von den befragten Experten generell ein hoher bis sehr hoher Schutzbedarf gesehen. Nach deren Meinung kann diesem Schutzbedarf durch Einhaltung der Regelungen des BSI IT-Grundschutz-Kompendiums entsprochen werden. Die Verschlüsselung der übermittelten Daten, zur Gewährleistung der Vertraulichkeit und Integrität, sowie die Authentifizierung der Nutzer bzw. Endgeräte, für die Gewährleistung der Authentizität der Daten, wird aus Expertensicht für grundlegend gehalten.

Bezüglich der erforderlichen Maßnahmen wurden von den befragten Experten unterschiedliche Wege aufgezeigt. Eine Position [23, 26, 59] besteht darin, dass dem Schutzbedarf nur durch eine eigene (behördliche) IKT-Infrastruktur entsprochen werden kann. Eine weitere Position [14] ist dadurch gekennzeichnet, dass entweder sehr hohe Sicherheitsauflagen an die Nutzung einer kommerziellen IKT-Infrastruktur durchzusetzen sind oder eine behördliche Infrastruktur aufgebaut werden muss. Ein weiterer Experte [15] nimmt die Position ein, dass die finanziellen Ressourcen, die für eine behördliche IKT-Infrastruktur notwendig wären, in die kommerzielle IKT-Infrastruktur investiert werden sollten, um dort hohe Sicherheitsstandards zu gewährleisten.

Als wesentlicher Schwachpunkt mobiler Breitbandanwendungen wurden von den befragten Experten für IT- und Informationssicherheit [59] die Endkomponenten von IoT-Geräten benannt. Diese von Unternehmen der Regelungs- und Steuertechnik entwickelten Sensoren weisen i.d.R. nicht die erforderliche Hardwareausstattung auf, um die BSI-Standards umsetzen zu können. Als Konsequenz werden z.B. im Hamburger Hafen, als Teil des KRITIS-Sektors, keine Entscheidungen getroffen, die ausschließlich auf Daten von IoT-Komponenten basieren. Bezogen auf die nichtpolizeiliche Gefahrenabwehr ist es daher ein entscheidender Aspekt, wie IoT-Daten in einen Entscheidungsprozess einfließen. Können die IoT-Daten den Entscheidungsprozess, z.B. der Einsatzleitung, maßgebend beeinflussen, muss die Datenquelle höchsten Sicherheitsstandards genügen.

In der gegenwärtigen Situation ist die Nutzung einer kommerziellen IKT-Infrastruktur unerlässlich, wenn Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr eingesetzt werden sollen. Die befragten IT-Experten sind sich einig, dass zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit von Daten zumindest ein virtuell privates Kommunikationsnetz (VPN) genutzt werden muss, wenn als Transportmedium ein kommerzielles Mobilfunknetz genutzt wird. Dies wird nach Auffassung der Experten [15, 59] erst entbehrlich, wenn der Mobilfunkstandard 5G nutzbar ist.

Mit dem 5G-Standard werden laut BSI deutlich strengere Sicherheitskriterien verbunden sein, als bei älteren Mobilfunknetzen (3G, 4G/LTE). Erstmalig werden anerkannte Sicherheitsnachweise für die sicherheitsrelevanten Komponenten eines Mobilfunknetzes verpflichtend eingeführt, die vom BSI geprüft und verantwortet werden. [60] Über das sogenannte „Network Slicing“ können virtuelle Netzwerke oder Dienste auch im Hinblick auf kurze Reaktionszeiten oder hohe Sicherheit gestaltet werden. Ein Experte für Informationssicherheit [59] gibt jedoch zu bedenken, dass die Netzbetreiber für einen gewissen Zeitraum eine Abwärtskompatibilität gewährleisten müssen, wodurch Lücken in der Sicherheitsarchitektur des 5G-Netzes zu erwarten sind.

4.3 Ausfallsicherheit

Ein ausfallsicheres Informations- und Kommunikationsnetz ist im Rahmen der nichtpolizeilichen Gefahrenabwehr unerlässlich, um effizient und sicher agieren zu können. Darüber herrscht in Fachkreisen Einigkeit. Bei den Experteninterviews wurden als **Ausfallszenarien** im Wesentlichen Angriffe von Dritten (physisch/virtuell), ein langanhaltender und großflächiger Stromausfall sowie eine Netzüberlastung genannt. Die Literaturauswertung ergab hierzu folgende Sachverhalte.

Im kommerziellen Übertragungsnetz des IKT-Sektors sind große Redundanzen gegeben. Ein langanhaltender und großflächiger Ausfall des IKT-Sektors, durch gezielte Angriffe, gilt nach einer Studie des BSI daher als unwahrscheinlich, falls nicht zentrale Metropolregionen ausfallen. Allerdings besteht eine große Abhängigkeit vom Energiesektor, insbesondere von der Stromversorgung. [52, S. 109]

Nach einer vom „Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag“ (TAB) veröffentlichten Studie [61] kommen als Ursachen für einen langandauernden

und regional übergreifenden Stromausfall u. a. technisches und menschliches Versagen, kriminelle Aktionen oder Extremwetterereignisse infrage. Es wird erwartet, dass die Ausfallwahrscheinlichkeit künftig größer wird. [61, S. 9] Das TAB kommt ferner zu dem Schluss: *„Die Folgen eines großräumigen, langfristigen Stromausfalls für Informationstechnik und Telekommunikation müssen als dramatisch eingeschätzt werden. Telekommunikations- und Datendienste fallen teils sofort, spätestens aber nach wenigen Tagen aus.“* [61, S. 9] Eine nachhaltige Absicherung der Kommunikationsnetze dürfte nach Auffassung des TAB weder wirtschaftlich noch technisch zu realisieren sein. [61, S. 11]

In Bezug auf das Ausfallszenario Netzüberlastung ist das Post- und Telekommunikationssicherstellungsgesetz (PTSG) [62] zu berücksichtigen. Nach § 6 Absatz 2 PTSG sind Behörden des Bundes, der Länder, der Gemeinden und Gemeindeverbände sowie Katastrophenschutz-, Zivilschutz- und Hilfsorganisationen, Hilfs- und Rettungsdienste telekommunikationsbevorrechtigt.

Die technischen Randbedingungen zur Umsetzung der Telekommunikationsbevorrechtigung sind in der Verfügung Nr. 57/2013 [63] der Bundesnetzagentur beschrieben. Dort ist zudem vermerkt: *„Vor dem Hintergrund immer kürzerer Innovationszyklen in der Mobilfunktechnik behält sich die Bundesnetzagentur vor, im Bedarfsfall ab dem Jahr 2020 die Festlegungen für die Bevorrechtigung von Datenübermittlungsdiensten auf Basis gewonnener Erfahrungen aus Krisensituationen zu überprüfen.“*

Somit kann das Ausfallszenario eines langanhaltenden und großflächigen Stromausfalls, das von allen Experten benannt wurde, als kritisches Ereignis herausgestellt werden.

Wie schon in Bezug auf das Schutzziel der Datenverfügbarkeit (Kapitel 4.2) angemerkt, werden von den befragten Experten teils unterschiedliche Positionen vertreten. Um der Möglichkeit des Ausfalls kommerzieller Mobilfunknetze infolge eines Stromausfalls zu begegnen, wurden eine behördliche IKT-Infrastruktur [23, 26, 59] oder staatliche Investitionen in die kommerzielle IKT-Infrastruktur als Möglichkeit genannt. [15] Experten aus dem KRITIS-Bereich [59] weisen darauf hin, dass in ihrem Sektor (Hamburger Hafen) kommerzielle Mobilfunknetze, u.a. aus Gründen der Ausfallsicherheit, nur als Rückfallstufe genutzt werden.

Bezüglich des Ausfalls kommerzieller IKT-Infrastruktur infolge einer Netzüberlastung wurde von Experten [15, 59] eine „Quality of Standard“-Vereinbarung vorgeschlagen. Diese ist bereits Bestandteil der Verfügung Nr. 57/2013 [63] der Bundesnetzagentur. In Bezug auf den Vorschlag redundanter Mechanismen [19] kann auf die Studie der BSI [52] verwiesen werden, wonach im kommerziellen Übertragungsnetz des IKT-Sektors große Redundanzen gegeben sind.

Als aussichtsreiche Entwicklung wird von mehreren Experten [15, 59], auch in Bezug auf die Ausfallsicherheit, die geplante Einführung des Mobilfunkstandards 5G angesehen, mit dem entsprechende Absicherungsmechanismen verbunden sein sollen.

4.4 Schlussfolgerung

Zur Nutzung von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr wird für einen nicht näher bestimmbaren Zeitraum die Verwendung kommerzieller IKT-Infrastrukturen erforderlich sein. Die Einführung des Mobilfunkstandards 5G weckt hierbei viele Erwartungen in Bezug auf Daten- und Ausfallsicherheit. Es ist jedoch nicht zu erwarten, dass das Szenario eines Ausfalls der kommerziellen IKT-Infrastruktur infolge eines langandauernden und großflächigen Stromausfalls hierdurch ausgeschlossen wird.

Ein Verzicht auf Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr wegen Vorbehalten gegenüber der Daten- und Ausfallsicherheit kann jedoch nicht als angemessene Reaktion betrachtet werden, da hierdurch eine zeitgemäße Entwicklung der BOS verhindert werden würde. Somit müssen die Einheiten der nichtpolizeilichen Gefahrenabwehr Strategien entwickeln, wie bei einem Komplett- oder Teilausfall kommerzieller IKT-Strukturen deren Handlungsfähigkeit erhalten bleibt.

Da im kommerziellen IKT-Sektor Sprach- und Datendienste über die gleichen technischen Komponenten transportiert werden, besteht die Gefahr, dass bei einer Störung der Netze Sprach- und Datendienste ausfallen. Solange das BOS-Digitalfunknetz funktionsfähig ist, können Sprachmitteilungen als geeignete Rückfallebene berücksichtigt werden. Eine Aufgabe des TETRA-Netzes kann aus Sicht des Verfassers erst in Betracht gezogen werden, wenn ein IKT-Netz zur Verfügung steht, welches mindestens den gegenwärtigen Sicherheitsstandards (TETRA) entspricht.

Die Möglichkeit der Bevorrechtigung innerhalb kommerzieller IKT-Netze nach PTSG ist für die Nutzung von Breitbandanwendungen durch die BOS essentiell. Allerdings können nicht bevorrechtigten Nutzer im Extremfall nur Notrufe über die Nummern 110 und 112 absetzen, jedoch keine Daten senden oder empfangen. Dies bedeutet, dass eine zeitgerechte Warnung der Bevölkerung über Anwendungen wie NINA oder KATWARN ggf. ausgeschlossen ist. Auch die Notruf-App, die den Zugang behinderter Endnutzer zu Notrufdiensten sicherstellen soll, wäre dann inaktiv. Dieser Sachverhalt muss bei einer Fortschreibung der Regelwerke aus Sicht des Verfassers mit hoher Priorität verfolgt werden. Entsprechende Pläne werden bei der Überarbeitung des „European Electronic Communications Code“ bereits verfolgt.

5 Fazit und Ausblick

"Die Digitalisierung schreitet rasch voran. Die Anzahl vernetzter Gegenstände in der Wirtschaft, aber auch im Alltag jedes Einzelnen wächst stetig. Zukünftig kommunizieren weltweit Milliarden Gegenstände, Sensoren oder Maschinen miteinander. Das Konsumenten-Internet erweitert sich zum Industrie-Internet. (...) Gebietskörperschaften sollen (…) Nachfrager und Anbieter von Konnektivität und technischen Komponenten zusammenführen, um gemeinsam Potenziale (...) zu erforschen." [64]

Dieses Zitat aus einer Bekanntmachung des BMVI vom 15.07.2019 zeigt deutlich, welcher Innovationswille von den politischen Verantwortlichen aktuell postuliert wird, um im globalen Wettbewerb schritthalten zu können.

Mit der fortschreitenden Vernetzung der Gesellschaft, die hier im Fokus steht, nimmt auch deren Vulnerabilität zu. Es besteht jedoch ebenso die Möglichkeit, durch eine stärkere Vernetzung der BOS, das erforderliche Maß an Sicherheit zu gewährleisten. Politik und Gesellschaft sollten sich auch dieser Herausforderung stellen.

Die Basis dieser digitalen Welt der Zukunft ist eine leistungsfähige und resiliente IKT-Infrastruktur, die allen, überall und jederzeit zur Verfügung steht. Insbesondere im Gefahrenfall muss sie das Netz bieten, um die zu erwartenden gesellschaftlichen Risiken [65] auffangen zu können. Ohne ein entsprechendes Mobilfunknetz wird Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr nur eine nachrangige Rolle zugesprochen können, wodurch weite Teile des Potentials einer digitalen Gesellschaft ungenutzt blieben.

Im Gegensatz zur Situation in Deutschland, wo die Mobilfunkstrategie der Bundesregierung die Belange des staatlichen Mobilfunks der BOS explizit ausschließt [6], wurde in den Vereinigten Staaten von Amerika 2012 ein Gesetz verabschiedet, dass den landesweiten Ausbau eines Breitbandnetzes festlegt, welches zur Gewährleistung der öffentlichen Sicherheit genutzt werden soll. [66] Das Gesetz steht in Zusammenhang mit der Aufarbeitung von 9/11 und damit mit einem Ereignis, das auch die nichtpolizeiliche Gefahrenabwehr tief erschüttert hat.

Auf Grundlage dieses Gesetzes wurde die „First Responder Network Authority“ (FirstNet), eine unabhängige Einrichtung, die zur National Telecomunication and Information Administration (NTIA) gehört, gegründet. Die FirstNet wurde autorisiert, eine öffentlich-private-Partnerschaft mit AT&T einzugehen, um ein die gesamten Vereinigten Staaten von Amerika umspannendes, dediziertes Breitbandnetz aufzubauen, das von Sicherheitsorganisationen genutzt werden kann. Hierbei ist es AT&T erlaubt, Kapazitäten, die aktuell nicht von Sicherheitsorganisationen benötigt werden, kommerziell zu nutzen. [43]

Die FirstNet-Infrastruktur bietet den Nutzern u.a. einen vorrangigen Zugriff auf Hochgeschwindigkeitsnetze, standortbasierte Dienste und Anwendungen für das Notfallmanagement. Hierbei stehen Zuverlässigkeit, Sicherheit und Redundanz im Fokus des Angebots. FirstNet sammelt zudem Eingaben von Sicherheitsorganisationen zu hilfreichen Breitbandanwendungen und gibt den Anwendern die Möglichkeit, Applikationen im FirstNet-Labor zu testen. Erprobte Applikationen werden in Bezug auf Cybersicherheit optimiert und anschließend einem breiten Anwenderkreis zur Verfügung gestellt. [66, S. 23]

Weitere dedizierte Breitbandnetze für Sicherheitsorganisationen sind in Südkorea (SafeNet), Australien (PSMB) und Frankreich (PCSTORM) im Aufbau bzw. in Betrieb. Im Vereinigten Königreich (UK) und Finnland werden von Sicherheitsorganisationen mobile Breitbandnetze genutzt, die nicht auf ein dediziertes Frequenzspektrum zurückgreifen. [67] Das in Finnland genutzte Breitbandnetz für BOS bzw. PPDR greift u.a. auf gehärtete Mobilfunknetze kommerzieller Anbieter und mobile Basisstationen zurück. [68]

Um den BOS die Nutzung von kommerziellen Breitbandnetzen zu ermöglichen, wurden und werden bei der Standardisierung des Mobilfunks (4G und 5G) „Critical Communication Functions“ definiert, wie z.B. einen „Fallback Modus“ der Basisstationen und die Realisierung von Gruppenrufen mit unterschiedlichen Prioritäten. Vollständig standardisierte und getestete Systeme stehen derzeit jedoch noch nicht zur Verfügung. Zunächst bleibt das TETRA-Digitalfunknetz daher das einzige System, das alle Leistungsmerkmale aufweist, die für eine einsatzkritische Kommunikation und Informationsübermittlung benötigt werden. [34]

Leitstellen der BOS wird künftig eine weitaus größere Bedeutung zukommen als bislang. Neben der Entgegennahme von Notrufen und der Alarmierung von Einsatzkräften wird das Datenmanagement an Bedeutung gewinnen. [26] Im Kontext einer „Smart City“ werden zudem Zentralen etabliert werden müssen, in denen der „digitale Puls“ einer Stadt überwacht wird, um bei Unregelmäßigkeiten zeitgerecht eingreifen zu können. Als Beispiel ist das „Operations Center“ der Küstenmetropole Rio de Janeiro zu nennen, in dem ständig 17 Kommunalbehörden und sieben staatliche Einrichtungen vertreten sind, darunter die Feuerwehr, der Rettungsdienst und der Katastrophenschutz. [69]

Um den Herausforderungen einer digitalen Gesellschaft zu begegnen und deren Potential zu nutzen, müssen Technik, Team und Taktik der nichtpolizeilichen Gefahrenabwehr darauf ausgerichtet werden, eine vorausschauende Gefahrenabwehr zu praktizieren. Hierfür ist eine Prozessanalyse erforderlich, um Optimierungsmöglichkeiten aufzuzeigen. Das Analyseergebnis könnte auf einer Plattform veröffentlicht werden, auf die Entwickler zugreifen, um Lösungen anzubieten. Ein Modell hierfür existiert in Berlin. Unter der Schirmherrschaft des Bundeskanzleramtes gründete ein Computerwissenschaftler das Unternehmen „Tech4Germany“, um die im Koalitionsvertrag formulierten Digitalisierungsziele der Bundesregierung zu unterstützen. [70, 70, 71]

Wenn die BOS ihre Kräfte bündeln, Experten einbeziehen und eine Plattform schaffen, um Breitbandanwendungen zu entwickeln, kann das erforderliche Potential entfesselt werden, um den Herausforderungen der nichtpolizeiliche Gefahrenabwehr auch in Zukunft gerecht zu werden. Das Leitthema der Interschutz 2020 „Der Blick in die vernetzte Zukunft“ bietet sich an, um dort erste gemeinsame Schritte zu machen.

Literaturverzeichnis

[1] o.V., *Breitband-Internetanschlüsse.* [Online] Verfügbar unter: http://www.destatis.de/Migration/DE/ZahlenFakten/LaenderRegionen/Internationales/Thema/ErlaeuterungenGlossar/BreitbandInternetanschluesse.html.

[2] o.V., „Konzept zur Durchführung von Eignungstests von Breitbandtechnologien für Behörden und Organisationen mit Sicherheitsaufgaben (BOS)“, Ständige Konferenz der Innenminister und -senatoren der Länder, Berlin, Jul. 2018. [Online] Verfügbar unter: https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/20181128_30/anlage-zu-top-42.pdf?__blob=publicationFile&v=2. Zugriff am: Nov. 28 2019.

[3] F. Tenzer, *Durchschnitliche Verbindungsgeschwindigkeit der Internetanschlüsse in den führenden Ländern weltweit im 1. Quartal 2017: Downstream-Geschwindigkeit.* [Online] Verfügbar unter: http://www.de.statista.com/statistik/daten/studie/224924/umfrage/internet-verbindungsgeschwindigkeiten-in-ausgewaehlten-weltweiten-laendern/. Zugriff am: Dez. 11 2019.

[4] o.V., „Digitalisierung gestalten: Umsetzungsstrategie der Bundesregierung“, Bundesregierung, Sep. 2019. [Online] Verfügbar unter: https://www.bundesregierung.de/breg-de/themen/digital-made-in-de. Zugriff am: Nov. 28 2019.

[5] A. Merkel und O. Scholz, „Pressekonferenz von Bundeskanzlerin Merkel und Bundesminister Scholz am 18. November 2019 in Meseberg: Mitschrift Pressekonferenz“, Bundesregierung, Nov. 2019. [Online] Verfügbar unter: https://www.bundesregierung.de/breg-de/aktuelles/pressekonferenz-von-bundeskanzlerin-merkel-und-bundesminister-scholz-am-18-november-2019-1693682. Zugriff am: Nov. 22 2019.

[6] o.V., „Eckpunkte einer Mobilfunkstrategie der Bundesregierung“, Bundesministerium für Verkehr und digitale Infrastruktur, Okt. 2019. [Online] Verfügbar unter: http://www.bmvi.de/ShareDocs/DE/Anlage/DG/Eckpunkte-Mobilfunkstrategie.pdf?_blob=publicationFile. Zugriff am: Nov. 26 2019.

[7] A. Gegenfurtner, „Das bewegt den Digitalfunk BOS 2019: Austausch mit den Feuerwehrverbänden“. Berlin, Okt. 10 2019.

[8] o.V., *The Birth of Broadband: Frequently Asked Questions.* [Online] Verfügbar unter: http://www.itu.int/osg/spu/publications/birtofbroadband/faq.html. Zugriff am: Dez. 10 2019.

[9] W. Goldenits, „Mobilfunk und Gesundheit: Fakten und Informationen zur Technik, Forschung und Sicherheit“, Deutsche Telekom AG, 2017. [Online] Verfügbar unter: http://www.telekom.com/de/Verantwortung/klima-und-umwelt/mobilfunk-und-gesundheit. Zugriff am: Dez. 12 2019.

[10] o.V., *Breitbandtechnik.* [Online] Verfügbar unter: http://www.elektronik-kompendium.de/sites/kom/1304161.htm. Zugriff am: Dez. 12 2019.

[11] H. A. Mieg und B. Brunner, „Experteninterviews: Eine Einführung und Anleitung“. MUB-Working Paper 6, Mensch- und Umweltbeziehungen, ETH, Zürich, 2001.

[12] T. Dresing und T. Pehl, *Praxisbuch Interview, Transkription & Analyse.: Anleitungen und Regelsysteme für qualitativ Forschende.,* 8. Aufl. Marburg, 2018.

[13] W. Schäuble, "Notfallkommunikation bei Stromausfällen: Initiative der „Versorger-Allianz 450“, Stellungnahme der AGBF Bayern", Brief, Jun. 2019.

[14] Experte D, *Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr*.
[15] Experte C, *Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr*.
[16] o.V., „Study of use cases and communications involving IoT devices in provision of emergency situations“, European Telecommunications Standards Institute, Sophia Antipolis Cedex ETSI TR 103 582, Jul. 2019.
[17] *Informations- und Kommunikationstechnik im Einsatz*, FwDV / DV 800, 2017.
[18] Dudenredaktion. [Online] Verfügbar unter: http://www.duden.de/node/179173/revision/179209. Zugriff am: Nov. 29 2019.
[19] Experte E, *Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr*.
[20] Initiative D21 e.V., Hg., *D21 Digitalindex 2018/2019: Jährliches Lagebild zur Digitalen Gesellschaft*. Online Paper, 2019.
[21] Dudenredaktion. [Online] Verfügbar unter: http://www.duden.de/node/81415/revision/81451. Zugriff am: Nov. 29 2019.
[22] o.V., *Fernmeldetaktik.* [Online] Verfügbar unter: http://www.lfs-bw.de/Fachthemen/Digitalfunk-Funk/Seiten/fernmeldetaktik.aspx. Zugriff am: Nov. 29 2019.
[23] Experte A, *Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr*.
[24] N. Barth *et al.,* „Kooperative Leitstelle - Modell der Zukunft: Projektarbeit am Beispiel Schleswig-Holstein“. Projektarbeit, Organisation und Projektmanagement, Fachhochschule Köln, Köln, 2009.
[25] K. Maurer, „Leitstelle der Zukunft: Transformation zum Dienstleister für operative Gefahrenabwehr und Informationsmanagement“, Arbeitsgemeinschaft der Leiter der Berufsfeuerwehren in der Bundesrepublik Deutschland, Mrz. 2017.
[26] Experte B, *Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr*.
[27] C. Schneider, „VIDal: Vernetzung von Informationen zur Darstellung der Landeslage“, Feuerwehr Bonn, 2019.
[28] o.V., „Leitstelle der Zukunft: Transformation zum Dienstleister für operative Gefahrenabwehr und Informationsmanagement“, Behörde für Inneres Sport - Feuerwehr, Jan. 2017.
[29] *Informations- und Kommunikationstechnik im Einsatz*, FwDV 800, 2017.
[30] G. Konrad und T. Hensel, „Mobile Einsatzstellenaufklärung: Einsatz von Drohnen“. Hamburg, Nov. 15 2019.
[31] o.V., *Wie Technik half, die Notre Dame zu retten: Hoffnungsträger Technik.* [Online] Verfügbar unter: https://www.ingenieur.de/technik/fachbereiche/bau/wie-technik-half-die-notre-dame-zu-retten/. Zugriff am: Dez. 02 2019.
[32] W. Kaczorowski, *Die smarte Stadt. Den digitalen Wandel intelligent gestalten: Handlungsfelder, Herausforderungen, Strategien*. Stuttgart, München, Hannover, Berlin, Weimar, Dresden: Richard Boorberg Verlag GmbH & Co KG, 2014.
[33] D. Aschenbrenner, „Feuerwehr 4.0: Welche Herausforderungen erwarten uns?“. Hamburg, Dez. 4 2017.
[34] M. Lampe, *PMR: Missionskritische Anwendungen in zukünftigen Mobilfunknetzen.* [Online] Verfügbar unter: http://www.doksystem.de/beitrag/items/pmr-missionskritische-anwendungen. Zugriff am: Dez. 11 2019.
[35] M. Weixlbaumer, „syBOS: 2. Alarmierungsweg - APP Alarmierung“. Hamburg, Nov. 15 2019.
[36] U. Nußbaum, „Kleine Anfrage der Abgeordneten Anke Domscheit-Berg, Dr. Petra Sitte, Simone Barrientos, weiterer Abgeordneter und der Fraktion DIE

LINKE BT-Drucksache: 19/6880: betr.: „Notruf-App für Menschen mit Behinderung"“, Bundesministerium für Wirtschaft und Energie, Jan. 2019. [Online] Verfügbar unter: http://www.bmwi/Redaktion/DE/Parlamentarische-Anfragen/2019/19-6880.pdf?_blob=publicationFile&v=8. Zugriff am: Dez. 02 2019.

[37] H. Lüdemann, „Mobile Breitbandanbindung ins Behördennetz für Einsatzfahrzeuge“. Hamburg, Nov. 14 2019.

[38] o.V., *Telenotarzt soll in Nordrhein-Westfalen landesweit eingeführt werden.* [Online] Verfügbar unter: http://www.äerzteblatt.de/nachrichten/103168/Telenotarzt-soll-in-Nordrhein-Westfalen-landesweit-eingefuehrt-werden. Zugriff am: Dez. 02 2019.

[39] F. Stadler, „Digitalisierung – Projekte und Prozesse bei der Feuerwehr: Workshop Jesteburg, Gründung Abteilung F06“. 17.10.2018, Jesteburg.

[40] O. Sartorius, „Generation Y: Eine Studie von TNS Infratest Politikforschung im Auftrag des Bundespresseamtes / BPA“, Berlin, Aug. 2015. [Online] Verfügbar unter: http://dbk.gesis.org/dbksearch/SDesc2.asp?no=6612&ll=10&af=1&db=d&search=&search2=&notabs=1&l=p&p=1.

[41] o.V., *Unfallerkennung und Notfallbenachrichtigung für Garmin-Uhren verfügbar.* [Online] Verfügbar unter: http://gps.de/unfallerkennung-und-notfallbenachrichtigung/. Zugriff am: Dez. 03 2019.

[42] o.V., *SmartSenior: Längere Selbstständigkeit von Seniorinnen und Senioren.* [Online] Verfügbar unter: http://www.smart-senior.de. Zugriff am: Dez. 03 2019.

[43] M. Ulema, *Fundamentals of Puplic Safety Networks and Critical Communications: Technologies, Deployment and Management,* 1. Aufl. Hoboken: John Wiley & Sons, 2019.

[44] C. Grant, A. Hamins, N. Bryner, A. Jones und G. Koepke, „Research Roadmap for Smart Fire Fighting: Summary Report“. NIST Special Publication 1191, National Institut of Standards and Technology - NIST, Mai. 2015. [Online] Verfügbar unter: http://www.dx.doi.org/10.6028/NIST.SP.1174. Zugriff am: Nov. 19 2019.

[45] U. Scharlack, *Zu gefährlich für Menschen? - Autonome Roboter helfen.* [Online] Verfügbar unter: https://www.bmbf.de/de/zu-gefaehrlich-fuer-menschen---autonome-roboter-helfen-8953.html. Zugriff am: Nov. 20 2019.

[46] o.V., *Internet of Things: At-a-glance.* [Online] Verfügbar unter: http://www.cisco.com/c/dam/en/us/products/colleteral/se/internet-of-things/at-a-glance-c45-731471.pdf. Zugriff am: Dez. 03 2019.

[47] A. Strüver, Hg., *Smart City: Kritische Perspektiven auf die Digitalisierung in Städten*. Bielefeld: transcript Verlag, 2018.

[48] S. Runkel, „Smarter Bevölkerungsschutz?: Risiko- und Sicherheitskommunikation zwischen Warnung und Werbung.“ in *Smart City: Kritische Perspektiven auf die Digitalisierung in Städten*, A. Strüver, Hg., Bielefeld: transcript Verlag, 2018, S. 127–137.

[49] o.V., *Schutz Kritischer Infrastrukturen: Bedeutung Kritischer Infrastrukturen für unsere moderen Gesellschaft.* [Online] Verfügbar unter: http://www.bsi.bund.de/DE/Themen/KRITIS/Strategie/KRITIS/kritischeinfrastrukturen_node.html. Zugriff am: Dez. 04 2019.

[50] S. Patig, A. Zwanziger und S. Herden, *IT-Infrastruktur.* [Online] Verfügbar unter: http://www.enzyklobaedie-der-wirtschaftsinformatik.de/lexikon/daten-wissen/Informationsmanagement/IT-Infrastruktur/index.html. Zugriff am: Dez. 04 2019.
[51] o.V., *Telekommunikationsinfrastrukturen.* [Online] Verfügbar unter: www.breitband-bautzen.de/index.php/faq?catid=4. Zugriff am: Dez. 04 2019.
[52] W. Dolle und P. Weissmann, „KRITIS-Sektorstudie: Informationstechnik und Telekommunikation (IKT)“. Öffentliche Version - Revisionsstand 5. Februar 2015, Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2015. [Online] Verfügbar unter: http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Sektorstudie_IKT.pdf?_blob=publicationFile. Zugriff am: Dez. 04 2019.
[53] S. Lenz, *Vulnerabilität Kritischer Infrastrukturen*. Bonn: BBK, 2009.
[54] o.V., *Was leistet der Digitalfunk BOS.* [Online] Verfügbar unter: http://www.bdbos.bund.de/SharedDocs/Meldungen/DE/2017/171128/_legenden.html. Zugriff am: Dez. 04 2019.
[55] o.V., *Drucksache 19/4233.* [Online] Verfügbar unter: http://www.dipbt.bundestag.de/dip21/btd/19/042/1904233.pdf.
[56] G. Bedürftig, *Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr*. Exploratives Telefoninterview. Bremen, Berlin.
[57] o.V., *IT-Grundschutz-Kompendium,* 2. Aufl. Köln: Bundesanzeiger Verlag GmbH, 2019.
[58] o.V., „Sicherheitsanforderungen: Netzelemente“. Deutsche Telekom Gruppe, Okt. 2016. [Online] Verfügbar unter: http://www.telekom.com/de/verantwortung/datenschutz- und datensicherheit/sicherheit/details/privacy-and-security-assesment-verfahren-342724. Zugriff am: Dez. 05 2019.
[59] Experte F, *Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr*.
[60] o.V., *Moderne Telekommunikationsinfrastrukturen (5G).* [Online] Verfügbar unter: http://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/5G/5G_node.html. Zugriff am: Dez. 05 2019.
[61] T. Petermann, H. Bradke, A. Lüllmann, M. Poetzsch und U. Riehm, *Was geschieht bei einem Blackout: Folgen eines langandauernden und großräumigen Stromausfalls*. Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag - 33. Berlin: Edition Sigma, 2011.
[62] *Gesetz zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen (Post- und Telekommunikationssicherstellungsgesetz - PTSG): Post- und Telekommunikationssicherstellungsgesetz - PTSG*, 2011.
[63] o.V., „Technische Festlegungen und zeitliche Vorgaben für die vorrangige Herstellung von Verbindungen im Mobilfunk für die Inanspruchnahme von Datenübermittlungsdiensten“, Amtsblatt der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen 22/2013.
[64] o.V., „Bekanntmachung der Förderrichtlinie „5G Innovationswettbewerb im Rahmen der 5x5G-Strategie““, Bundesministerium für Verkehr und digitale Infrastruktur, Berlin, Jul. 2019. [Online] Verfügbar unter: https://www.bmvi.de/SharedDocs/DE/Artikel/DG/5g-mobilfunk-zukunft.html. Zugriff am: Nov. 28 2019.

[65] o.V., *Umfrage zur Zunahme gesellschaftlicher Risiken in der Zukunft 2012.* [Online] Verfügbar unter: http://de.statista.com/statistik/daten/studie/240027/umfrage/befuerchtungen-gesellschaftlicher-bedrohungen-in-der-Zukunft/. Zugriff am: Dez. 12 2019.
[66] J. C. Gallagher, „The First Responder Network (FirstNet) and Next Generation Communications for Public Safety: Issues for Congress“, Congressional Research Service, Washington D.C., Apr. 2018. [Online] Verfügbar unter: http://www.fas.org/sgb/crs/homesec/R45179.
[67] S. Holen, „5G Vertical User Workshop: National plans and roadmaps towards broadband“. Brüssel, Februar 2019.
[68] B. Virkkunen, „Multi-Access mobile broadband service for PPDR users in Finland“, Ukkoverkot Oy, Nov. 2016. [Online] Verfügbar unter: http://www.ukkoverkot.fi. Zugriff am: Nov. 19 2019.
[69] C. Schreiner, „International Case Studies of Smart Cities: Rio de Janeiro, Brazil“, 2016. [Online] Verfügbar unter: http://publications.iadb.org/en/international-case-studies-smart-cities-rio-de-janeiro-brazil. Zugriff am: Nov. 07 2019.
[70] o.V., *Für einen digitaleren Staat: Wir sind Deutschlands Technologie-Taskforce und machen die Bundesregierung und Verwaltung fit für die Digitalisierung!* [Online] Verfügbar unter: http://www.tech4germany.ort. Zugriff am: Dez. 09 2019.
[71] S. Soares, *Deutschlands Chefdigitalisierer: Der wichtigste Job von Kanzleramtsminister Helge Braun.* [Online] Verfügbar unter: https://www.manager-magazin.de/premium/helge-braun-kanzleramtsminister-soll-deutschland-digitalisieren-a-00000000-0002-0001-0000-000161978247. Zugriff am: Dez. 09 2019.

Tabellenverzeichnis

Abkürzungsverzeichnis

3GPP	3rd Generation Partnership Projekt, weltweite Kooperation von Gremien für die Standardisierung im Mobilfunk
2/3/4/5G	Mobilfunkstandard der 2./3./4./5. Generation
AER	Automated Emergency Response
AGBF	Arbeitsgemeinschaft der Leiter der Berufsfeuerwehren
AT&T	Nordamerikanischer Telekommunikationskonzern
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
BIM	Building Information Modeling beschreibt eine Methode der vernetzten Planung, Ausführung und Bewirtschaftung von Gebäuden
BMBF	Bundesministerium für Bildung und Forschung
BMVI	Bundesministerium für Verkehr und Innovation
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BSI	Bundesamtes für Sicherheit in der Informationstechnik
BSPP	Brigade de Sapeurs-Pompiers de Paris
CBRN	Chemical, Biological, Radiological and Nuclear
CISCO	US-amerikanisches Telekommunikationsunternehmen
DV	Dienstvorschrift
EC	Emergency Calling
ETSI	European Telecommunications Standards Institute
FHD	Full High Definition, Videoauflösung von 1.920 x. 1.080 Pixel
FwDV	Feuerwehr-Dienstvorschrift
GIS	Geographische Informationssysteme
GSM	Global System for Mobile Communications, Mobilfunkstandard der 2. Generation
HDTV	High Definition Television, hochauflösendes Fernsehen
IKT	Information- und Kommunikation

IoT	Internet of Things
IP	Internet Protocol, technologische Grundlage des Internets
ISDN	Integrated Services Digital Network, Standard für TK-Netz
ITU	International Telecommunications Union
KATWARN	Warn- und Informationssystem für die Bevölkerung
KI	Künstliche Intelligenz
KRITIS	Kritische Infrastruktur
KVK	Karlsruher Virtueller Katalog
LTE	Long Term Evolution, Mobilfunkstandard der 3. Generation
MANV	Massenanfall von Verletzten
MCC	Mission Critical Communications
MCD	Mission Critical Data
NINA	Notfall-Informations- und Nachrichten-App
NTIA	National Telecomunication and Information Administration
PPDR	Public Protection and Disaster Relief: Schutz der Öffentlichkeit und Katastrophenhilfe
PTSG	Post- und Telekommunikationssicherstellungsgesetz
PWS	Public Warning System
RATCOM	Réseau d'Alerte aux Tsunamis et submersions Côtières en Méditerranée
TAB	Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag
TETRA	Terrestrial Trunked Radio, Standard des Digitalfunk der BOS
TK	Telekommunikation
UHD	Ultra High Definition, Videoauflösung von 3.840 x 2.160 Pixel
vfdb	Vereinigung zur Förderung des Deutschen Brandschutzes
VoIP	Voice over IP, Sprachkommunikation in einem IP-Netzwerk
VPN	Virtual Private Network

Anhang

A Experteninterview – Gesprächspartner

Institution	Ansprechpartner	Funktion
IMK: AG Breitband **Bundesministerium des Innern:** BDBOS	Dr. Gerald Bedürftig	Leiter der AG Breitband Referatsleiter Kernnetz-, Schnittstellen- und Dienstrealisierung bei der BDBOS
Hamburg, Behörde für Inneres und Sport: Zentralstelle für den Digitalfunk der BOS	Eva-Maria Eckmann	Leiterin der Zentralstelle für den Digitalfunk
NRW, Ministerium des Innern: Referat 33	Dr. Klaus Block	Leiter der Arbeitsgruppe FwDV 800/810
Deutscher Städtetag: Arbeitsgemeinschaft der Leiter der Berufsfeuerwehren / Deutscher Feuerwehrverband, Fachausschuss Leitstellen und Digitalisierung	Jens Cordes	Vorsitzender des Fachausschusses
vfdb: Referat 7 „Informations- und Kommunikationstechnik **RXSK GmbH**	Stefan Truthän	Mitarbeiter im Referat 7, Chief Organisational Architect, CEO, Mitglied Berliner Feuerwehr (FF)
KRITIS: Hamburg Port Authority	Stefan van Eijden	Head of IT Operations & Infrastructure
KRITIS: Hamburg Port Authority	Dr. Quang-Vu Pham	Beauftragter für Datenschutz und Informationssicherheit
Explorative Interviews		
Hamburg, Behörde für Inneres uns Sport: F06 Informationsmanagement	Heiko Lüdemann	Informatiker, Arbeitsschwerpunkt Führungsunterstützungssysteme
IMK: AK II, AK V, Expertengruppe Leitstellen und Notruf	Carsten Schneider	Stellv. Leiter der Feuerwehr Bonn, Mitglied der Expertengruppe Leitstellen und Notruf im AK II und AK V der IMK

B Experteninterview – Fragen allgemein

Einstiegsfragen

1. Seit wann befassen Sie sich mit Breitbandanwendungen für die BOS?
2. In welchem Umfang haben Sie sich mit Breitbandanwendungen für die BOS befasst?
3. In welcher Funktion haben Sie sich mit Breitbandanwendungen für die BOS befasst?

Notwendigkeit von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr

4. Welche Potentiale können aus Ihrer Sicht durch die Nutzung von Breitbandanwendungen für die nichtpolizeiliche Gefahrenabwehr freigesetzt werden?
5. Welche Herausforderungen sind aus Ihrer Sicht mit der Nutzung von Breitbandanwendungen für die nichtpolizeiliche Gefahrenabwehr verbunden?
6. Welche Gründe sprechen aus Ihrer Sicht **für** die Nutzung von Breitbandanwendungen in der die nichtpolizeilichen Gefahrenabwehr?
7. Welche Gründe sprechen aus Ihrer Sicht **gegen** die Nutzung von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr?
8. Welche Arbeitsmittel müssen den Einsatzkräften der Generation Z aus Ihrer Sicht geboten werden, um deren Potential für die nichtpolizeilichen Gefahrenabwehr vollumfänglich nutzen zu können?
9. In welchem Umfang ist aus Ihrer Sicht eine Unterscheidung zwischen einsatzkritischer Kommunikation und nicht einsatzkritischer Kommunikation (Datenfunk) in der nichtpolizeilichen Gefahrenabwehr möglich? Welche Breitbandanwendungen würden Sie der Kategorie „einsatzkritische Kommunikation“ zuordnen?

Einsatzmöglichkeiten von Breitbandanwendung in der nichtpolizeilichen Gefahrenabwehr

10. Welche Einsatzmöglichkeiten von Breitbandanwendungen sind aus Ihrer Sicht in der nichtpolizeilichen Gefahrenabwehr **gegenwärtig** denkbar?
11. Welche Einsatzmöglichkeiten von Breitbandanwendungen sind aus Ihrer Sicht in der nichtpolizeilichen Gefahrenabwehr **zukünftig** denkbar?
12. In welchen Tätigkeitsbereichen kann aus Ihrer Sicht eine Optimierung der nichtpolizeilichen Gefahrenabwehr durch Breitbandanwendungen erreicht werden?
13. In welchem Umfang erwarten Sie eine Steigerung des Sicherheitsniveaus in der nichtpolizeilichen Gefahrenabwehr durch den Einsatz von Breitbandanwendungen?

Datensicherheit bei der Nutzung von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr

14. Welchen Schutzbedarf sehen Sie in Bezug auf die Datensicherheit bei der Nutzung von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr?
15. Wie bewerten Sie die Risiken in Bezug auf die Datensicherheit bei der Nutzung von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr?

16. Welche Sicherheitsstandards sollten aus Ihrer Sicht bei der Nutzung von Breitbandanwendungen in der nicht polizeilichen Gefahrenabwehr angewandt werden, um die Datensicherheit zu gewährleisten?
17. Welche technischen Maßnahmen sind aus Ihrer Sicht bei der Nutzung von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr erforderlich, um die Datensicherheit zu gewährleisten?
    a) Vertraulichkeit der Daten
    b) Integrität der Daten
18. Welche organisatorischen Maßnahmen sind aus Ihrer Sicht bei der Nutzung von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr erforderlich, um die Datensicherheit zu gewährleisten?
    a) Vertraulichkeit der Daten
    b) Integrität der Daten

Ausfallsicherheit bei der Nutzung von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr

19. Welche Szenarien für den Ausfall von Breitbandanwendungen in der nichtpolizeilichen Gefahrenabwehr sind aus Ihrer Sicht denkbar?
20. In welchem Umfang muss aus Ihrer Perspektive Rücksicht auf die Ausfallsicherheit mobiler Breitbandnetze für Nutzer außerhalb der BOS genommen werden (absetzen von Notrufen, kritische Infrastrukturen etc.)?
21. Welchen Schutzbedarf sehen Sie in Bezug auf den Ausfall von mobilen Breitbandnetzen bei einer Nutzung durch die BOS?
22. Wie bewerten Sie die Risiken in Bezug auf den Ausfall von mobilen Breitbandnetzen bei einer Nutzung durch die BOS?
23. Welche Maßnahmen sind aus Ihrer Sicht erforderlich, um eine dauerhafte und flächendeckende Verfügbarkeit mobiler Breitbandnetze für die BOS zu gewährleisten?
24. Welche Maßnahmen sind aus Ihrer Sicht erforderlich, um eine hinreichende Resilienz der mobilen Breitbandnetze und spezifischer Breitbandanwendungen für eine Nutzung durch die BOS zu gewährleisten?

Ausstiegsfragen

25. Welche weiterführenden Unterlagen sollten im Rahmen der Facharbeit aus Ihrer Sicht berücksichtigt werden?
26. Haben Sie Hinweise, die bei der weiteren Bearbeitung der Facharbeit berücksichtigen werden sollten?
27. Darf ich Sie zitieren?
28. Wünschen Sie eine die Anonymisierung Ihrer Daten?
29. Haben Sie Fragen an mich?

C Experteninterview – Fragen an KRITIS

Einstiegsfragen

1. Seit wann befassen Sie sich mit Breitbandanwendungen für den Hafen?
2. In welchem Umfang haben Sie sich mit Breitbandanwendungen für den Hafen befasst?
3. In welcher Funktion haben Sie sich mit Breitbandanwendungen für den Hafen befasst?

Einsatzmöglichkeiten von Breitbandanwendung im Hafen

4. Welche Einsatzmöglichkeiten von Breitbandanwendungen sind aus Ihrer Sicht **gegenwärtig** denkbar?
5. Welche Einsatzmöglichkeiten von Breitbandanwendungen sind aus Ihrer Sicht **zukünftig** denkbar?

Datensicherheit bei der Nutzung von Breitbandanwendungen Hafen

6. Welchen Schutzbedarf sehen Sie in Bezug auf die Datensicherheit bei der Nutzung von Breitbandanwendungen?
7. Wie bewerten Sie die Risiken in Bezug auf die Datensicherheit bei der Nutzung von Breitbandanwendungen?
8. Welche Sicherheitsstandards sollten aus Ihrer Sicht bei der Nutzung von Breitbandanwendungen angewandt werden, um die Datensicherheit zu gewährleisten?
9. Welche technischen Maßnahmen sind aus Ihrer Sicht bei der Nutzung von Breitbandanwendungen erforderlich, um die Datensicherheit zu gewährleisten?
10. Welche organisatorischen Maßnahmen sind aus Ihrer Sicht bei der Nutzung von Breitbandanwendungen erforderlich, um die Datensicherheit zu gewährleisten?

Ausfallsicherheit bei der Nutzung von Breitbandanwendungen im Hafen

11. Welche Szenarien für den Ausfall von Breitbandanwendungen sind aus Ihrer Sicht denkbar?
12. Welchen Schutzbedarf sehen Sie in Bezug auf den Ausfall von mobilen Breitbandnetzen?
13. Wie bewerten Sie die Risiken in Bezug auf den Ausfall von mobilen Breitbandnetzen?
14. Welche Maßnahmen sind aus Ihrer Sicht erforderlich, um eine hinreichende Resilienz der mobilen Breitbandnetze zu gewährleisten?

Ausstiegsfragen

15. Welche weiterführenden Unterlagen sollten im Rahmen der Facharbeit aus Ihrer Sicht berücksichtigt werden?
16. Haben Sie Hinweise, die bei der weiteren Bearbeitung der Facharbeit berücksichtigen werden sollten?
17. Darf ich Sie zitieren?
18. Wünschen Sie die Anonymisierung Ihrer Daten?
19. Haben Sie Fragen an mich?

D Experteninterview – Exzerpt

Notwendigkeit von Breitbandanwendungen – Herausforderungen

Experte	Stichworte
A	• Technik • Datensicherheit • Ausfallsicherheit • Organisation • Schulung • Akzeptanz • Nutzbarkeit
B	• Sicherheit- und Stabilität der Übertragungswege • Vertrauen in Stabilität und Sicherheit der Geräte / Anwendungen • Einsätze in Smart Home- und Smart City-Umgebungen (Gerätesteuerungen, Schließberechtigungen etc.)
C	• Sensibilisierung des Marktes • ganzheitliche Betrachtung (Technik, Team und Taktik) • Verhinderung einer „Schatten-IT“ aufgrund mangelnder staatlicher Infrastruktur (private Anwendungen werden dienstlich genutzt) • zu hohe Sicherheitsansprüche blockieren die Entwicklung • Vertrauen in Stabilität und Sicherheit der Geräte / Anwendungen • Berücksichtigung von Gesamtsystemen anstelle von Einzelanwendungen (Kapazitätsbedarf) • Datenflut/Datentransparenz
D	• Zuteilung eines geeigneten Frequenzbereiches für die BOS.
E	• Vereinheitlichung der Standards • Aufrechterhaltung der Handlungsfähigkeit bei Systemausfall • Entwicklung adaptiver Applikationen, die auch bei geringer Datenübertragung, zumindest in vereinfachter Form, noch funktionsfähig sind (Reduzierung der Bildauflösung etc.) • Blickwinkel für Gesamtsystem einnehmen, nicht nur für isolierte Anwendungen bzw. Nutzerkreise • Kapazitätsvorhersage
F	• Kein Beitrag

Notwendigkeit von Breitbandanwendungen – Chancen

Experte	Stichworte
A	• Medienbruchfreie Datenübertragung (ABC-Einsatz, medizinische Rettung, etc.) • Luftaufklärung von Leitstellen aus • Bildübertragung aus Gefahrenbereichen • Datennutzung • Nutzung des technischen Potentials • Steigerung der Arbeitssicherheit von Einsatzkräften • ressourcenschonender Einsatz von Mannschaft und Gerät • Einsatzdokumentation • Befriedigung des gesteigerten Informationsbedürfnisses vorgesetzter Stellen, der Presse und der Bevölkerung • Steigerung des Sicherheitsniveaus der Bevölkerung (KI) • Information von entfernten Entscheidungsträgern
B	• Steigerung der Wissensbasis für Entscheidungen, die für Leib- und Leben von Menschen maßgebend sind • Unterstützungsmöglichkeiten für Einsatzkräfte zur Steigerung der Sicherheit • Optimierung des Arbeitsalltags • Nutzung der Fähigkeiten des Personals zur Nutzung digitaler Anwendungen (Ressourceneffizienz) • Gezieltere und schnellere Gefahrenabwehr
C	• von der Einsatzstelle abgesetzte Stäbe, die auf Grundlage von Echtzeitinformationen Entscheidungen treffen • effizientes Update digitaler Einsatzmittel • Datenstreaming aus zentralem Datenpool • effizienterer Personaleinsatz durch Automatisierung von Steuerungsvorgängen (Pumpe etc.) • Kompensation gegebener Nachteile durch hohe Verkehrsdichten durch Echtzeitrouting für BOS
D	• Nutzung von Smart City Daten
E	• Schnellere und effizientere Abwicklung von Krisensituationen oder allgemeinen Arbeitssituationen • Nutzbarkeit von Fachanwendungen aus dem Arbeitsalltag, dadurch hohe Anwendungssicherheit
F	• Kein Beitrag

Einsatzmöglichkeiten von Breitbandanwendungen – Gegenwart

Experte	Stichworte
A	• Datenübertragung zwischen Messleitkomponenten und Messfahrzeugen im Rahmen des ABC-Schutzes ohne Medienbruch • Einsatz von Drohnen zur Bildübertragung während der Einsatzabwicklung • Bildübertragung von Trupps zu Einheitsführer • Nutzung von Objektplänen • Übermittlung von Patientendaten • Übermittlung von Vitaldaten von Einsatzkräften
B	• Datenaustausch zwischen Leitstellen, abgesetzten Einsatzleitungen und Stäben • Datenübertragung an Krankenhäuser (Patientendaten, Telemetrie, Brandbettenvermittlung etc.) • Übermittlung von Erkundungsergebnissen • Nutzung von Objektplänen • Gemeinsame Lagekartendarstellung an verschiedenen Orten • Digitale Katastrophenschutzpläne
C	• Videokonferenzen • Videostreaming durch Drohnen • Steuerung von Robotern etc. (Beispiel Notre Dame) • Telemedizin • Cloud-Computing • Nonverbale Einsatzstellenkommunikation
D	• Kein Beitrag
E	• Datenbankzugriffe • Datenkommunikation • Verkehrslenkung • Optimierung von Anfahrtswegen • Alarmierungsmechanismen • Übermittlung von Patientendaten • Internetzugang • Datenaustausch zwischen Leitstellen und Einsatzleitung
F	• Kein Beitrag

Einsatzmöglichkeiten von Breitbandanwendungen – Zukunft

Experte	Stichworte
A	• Einsatz von autonomen Drohnen zur Bildübertragung im Rahmen der Alarmierung • Einsatz von Robotik/Manipulatoren/Drohnen zur Übernahme von Arbeiten in gefährlichen oder für Menschen unzugänglichen Bereichen • Prognosemethoden zur Führerkennung von entstehenden Gefahrenlagen (Big-Data, KI)
B	• Entwicklung der Leitstellen zu Wissensbasen der nichtpolizeilichen Gefahrenabwehr • Erkundung durch Drohnen von Leitstellen aus • Einsatz von Robotik zur Übernahme von Arbeiten in gefährlicher Umgebung • Augmented Reality für Einsatzkräfte über Datenbrillen • Sensorische Schutzkleidung • Virtual Reality für die Aus- und Fortbildung • Kommunikation mit Gebäuden (Smart Home, Smart City, IoT) • Einsatz von KI zur Erweiterung des Wahrnehmungshorizonts von Einsatzkräften (Leitstelle Kopenhagen).
C	• Echtzeitdatenübertragung an Entscheidungsträger • Virtual Reality für die Aus- und Fortbildung • Erkundung durch Drohnen • zentrale und automatische Steuerung von Aggregaten auf Einsatzfahrzeugen • IoT (Strahlrohr zu Pumpe, Wasserdruck) • virtuelle Feuerwehr-Schließberechtigung im Kontext Smart Home (Public-Key-Infrastructure für Gebäude/Räume) • Echtzeit-Routing, • Holografie/AR zur Erkundung • Nutzung von Sensorik/KI zur Erkundung • IoT, z.B. Pairing Einsatzhandschuh mit Pumpe und damit Fernbedienung • Verarbeitung von Smart Home- / Smart City-Daten durch IoT-Technik in Feuerwehrfahrzeugen (automatisierte Personensuche, Übertragung der Standortdaten AR, Auswertung von Belegungsdaten von Hotels, Krankenhäusern etc.)
D	• Kein Beitrag
E	• Steuerung von Robotern und Drohnen • autonomes Fahren • Augmented Reality
F	• Kein Beitrag

Sicherheitsaspekte von Breitbandanwendungen – Datensicherheit

Experte	Stichworte
A	• Hackerangriffe (Einspielung falscher Daten) • auf ersten Blick geringe Sicherheitsrelevanz der Daten (nichtpolizeiliche Gefahrenabwehr), im gesamtstaatlichen Kontext jedoch hoher Schutzbedarf • Ende-zu-Ende-Verschlüsselung • Verschlüsselung der Luftschnittstellen • eigene Server • eigene Leitungen/Netz • materieller und organisatorischer Schutz vor Angriffen Dritter • automatisierte logische Überprüfung der Daten (KI) • leistungsfähiger Support für die digitale Infrastruktur
B	• Hackerangriffe / missbräuchliche Datennutzung • eigene Speicherkapazitäten erforderlich • eigene Übermittlungswege • Ende-zu-Ende-Verschlüsselung • Sensibilisierung der Mitarbeiter
C	• Hackerangriffe
D	• Gesichertes Netz erforderlich • hohe Sicherheitsauflagen an kommerzielle Betreiber oder eigenes Netz • Datenverschlüsselung
E	• Verschlüsselung • Entkopplung private und dienstliche Nutzung, wenn ein Gerät für beide Anwendungen genutzt werden soll
F	• IoT-Endkomponenten, wie Sensoren etc. gelten in Bezug auf den Datenschutz aus unsicher, da die üblichen Sicherheitsmaßnahmen aus technologischen Gründen nicht angewandt werden können (z.B. monatliches patchen von SPS-Technik zur Fehlerbeseitigung) • Verschlüsselung • 5G wird hohe Sicherheitsstandards bieten, wodurch VPN entbehrlich wird, wobei • Provider auch eine Abwärtskomptabilität sicherstellen müssen, wodurch wieder Angriffspunkte entstehen

Sicherheitsaspekte von Breitbandanwendungen – Ausfallsicherheit

Experte	Stichworte
A	• Netzüberlastung • Blackout • Extremwetterereignisse • Bauarbeiten im Bereich der Netzinfrastruktur • Kommunikation mit der Bevölkerung • Manipulationen Dritter an der Netzinfrastruktur • nationales Roaming (Zugriff auf alle verfügbaren Netze) • Beschränkung der Endgeräte
B	• Manipulation von Dritten an Netzkomponenten • staatliche Netze • Blackout/Stromausfall • Extremwetterereignisse • Netzüberlastung
C	• Standards für öffentliche Netze von staatlicher Seite vorgeben, anstatt in ein eigenes Netz zu investieren. Kapital kann in öffentliche Netze investiert werden (Härtung). • Blackout • QoS-Vereinbarung (Quality of Service)
D	• Härtungsmaßnahmen • Blick auf Komponentenherstellern erforderlich (der Staat darf von Herstellern nicht erpresst werden können) • Stromausfall • Netzüberlastung
E	• Stromausfall • Wassereinbruch • Erdbeben • Hackerangriffe • Manipulation der Infrastruktur • Störsender • Härtungsmaßnahmen • redundante Mechanismen
F	• 5G-Slicing • 5G-Standard beinhaltet Ausfallsicherheit • kommerzielles LTE-Netz nicht notstromversorgt • Extremwetterereignisse • Funkschatten • Jammer • Quality of Service • vollständige Netzabdeckung nur mit staatlichem Netz erreichbar • Staatliches Netz

Eidesstattliche Erklärung

Hiermit versichere ich, Alexander Wellisch, die vorliegende Arbeit selbständig, ohne fremde Hilfe und ohne Benutzung anderer als der von mir angegebenen Quellen angefertigt zu haben. Alle aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche gekennzeichnet.

Die Arbeit wurde noch keiner Prüfungsbehörde in gleicher oder ähnlicher Form vorgelegt.

Hamburg, 16.12.2019

.....

Alexander Wellisch

Datenträger