

# Vorbereitung und Voraussetzungen für digital arbeitende Teams

Das folgende Kapitel soll organisatorische und technische Anforderungen an VOST zusammenfassen und somit eine Grundlage für den Aufbau neuer VOST oder kleiner Monitoring-Einheiten, sowie zur Schulung neuer Mitarbeiter:innen bieten. Darüber hinaus bietet dieses Kapitel eine erste deutsche Zusammenfassung, der wissenschaftlich identifizierten Voraussetzungen und Erfahrungswerte.

Dabei beschreiben organisatorische Anforderungen Rahmenbedingungen, welche im Rahmen des Nutzungskontextes getroffen sein sollten, damit das interaktive und multipersonnelle System effizient umgesetzt werden kann. Hierzu zählen unter anderem die verschiedenen Status von VOST sowie spezifische Informationen zu Mitarbeiter:innen und deren Verknüpfung. Darüber hinaus sollen unter technischen Anforderungen auch die erforderliche Hard- und Software thematisiert werden. Das folgende Kap. Eigenschutz stellt als einen wesentlichen organisatorischen Schwerpunkt den technischen und psychischen Eigenschutz dar, welcher explizit bei der Tätigkeit in einem VOST berücksichtigt werden sollte, um die Arbeitsfähigkeit sicher zu etablieren und zu erhalten. Das gesamte vorliegende Kapitel fokussiert folglich den präventiven Ansatz zur Schaffung von Rahmenbedingungen, um die Arbeits- und Vorgehensweise zu strukturieren und zu koordinieren.

## Organisatorische Vorbereitung und Voraussetzungen von Virtual Operations Support Teams

Ein wesentlicher Unterschied von VOST zu Digital-Freiwilligen, die bei Organisationen wie dem Digital Humanitarian Network ehrenamtlich tätig sind, ist die (angestrebte) Einbettung in einer staatlichen Gefahrenabwehrbehörde (Fathi, 2019b). Hierfür sind verschiedene Bedingungen notwendig, um die formale Zusammenarbeit zwischen Behörde und Freiwilligenorganisation zu ermöglichen. Dazu zählen vor allem Anforderungen an die Teammitglieder sowie deren strukturelle Netzwerkverbindung. Darüber hinaus sind Mitglieder in einem VOST im Vergleich zu digitalen Spontanhelfer:innen in etablierten und konstanten Strukturen. Folglich besteht das Team auch über akute Einsatzlagen hinaus und weist damit verschiedene Status auf.

### Verschiedene Status des Teams

Zu diesen Status zählen der aktivierte, im Rahmen von akuten und geplanten Einsatzlagen, sowie der inaktivierte Zustand.

#### Inaktiverter Zustand

Außerhalb von akuten oder geplanten Einsatzlagen befinden sich die VOST im inaktivierten Zustand (Silver, 2024). Während dieser Phasen, welche den größten Zeitraum einnehmen, besteht die Möglichkeit, Strukturen zu etablieren oder zu festigen, Kompetenzen zu vertiefen oder zu vermitteln sowie interorganisationale Verknüpfungen zu erstellen oder zu erweitern. Folglich erfahren die

Führungskräfte in dieser Phase einen veränderten aber sehr wichtigen Aufgabenwandel, um die Zusammenarbeit und Qualität der Arbeit im Team zu stärken. Möglichkeiten hierzu können folgende sein:

- Durchführung interner Analyse-Projekte, (Über bspw. eine Analyse der aktuellen Stimmung der Bevölkerung in einem bestimmten Ort kann eine Basislinie der Stimmung für spätere Vergleiche im Einsatz ermittelt werden. Außerdem kann sie dazu beitragen, die methodischen Vorgehensweisen zu optimieren und die Verifizierungsprozesse zu beschleunigen.)
- Aktualisierung/Erstellung einer Übersicht über SoMe Plattformen, (bspw. Zugriffsmöglichkeiten, Nutzerkreise, Fokussierungen im Team, etc.)
- Zusammenfassung und Lernen aus dem aktuellen Forschungsstand, (bspw. Lernen aus wissenschaftlichen Erkenntnissen zu Befürchtungen von Entscheidungsträger:innen bei der Integration von Digital-Freiwilligen)
- Nachbesprechung und Aufarbeitung durchgeführter Einsätze, (bspw. Lessons Learned dokumentieren und notwendige Änderungen umsetzen)
- Erstellung/Aktualisierung einer Übersicht über aktive VOST und Netzwerken, (bspw. treu dem Motto \glqq vor der Lage Köpfe und Zuständigkeiten kennen\grqq{ } Kontaktierungsmöglichkeiten austauschen und Unterstützungsanfragen sowie Kooperationen abklären)
- Erstellung/Anpassung der öffentlichkeitswirksamen Kommunikation und Information, sowie, (bspw. Pflege der eigenen Accounts in SoMe oder Webseiten)
- Identifikation von Einsatzindikationen. (bspw. Erweiterung des eigenen Portfolios und Beschreibung, bei welchen Szenarien eine Alarmierung erfolgen kann)

Im [Anhang](#) werden beispielhafte Einsatzaufträge für den inaktivierten Zustand aufgeführt, welche für eine interne „Aktivierung“ des eigenen Teams verwendet werden können. Die interne „Aktivierung“ kann dadurch sowohl notwendige Ergebnisse produzieren, als auch ein Übungs-Setting für die Mitglieder schaffen und den Zusammenhalt innerhalb eines Teams stärken. Neben den Übungs-Settings im inaktivierten Zustand sollten auch wiederkehrende, digitale Team-Meetings anvisiert werden, welche für Fortbildungen (Vorträge von Externen, anderen VOST oder internen Mitgliedern) oder zum allgemeinen Austausch genutzt werden können.

## Aktivierter Zustand

Aufbauend auf den gebildeten Strukturen ist ein VOST somit kurzfristig aktivierbar und kann bei geplanten sowie ungeplanten/plötzlich auftretenden Ereignissen zur Unterstützung der Lagekoordination eingesetzt werden. Anfordernde Stellen sind dabei Feuerwehr und Polizei sowie Krisen- und Einsatzstäbe von Ländern, Kreisen und Kommunen (Fathi, 2021). Der Einsatzauftrag muss dabei konkret formuliert werden, um eine effiziente und zielgerichtete Tätigkeit zu ermöglichen, die eine digitale Lageerkundung und folglich eine verbesserte Entscheidungsgrundlage ermöglicht, siehe auch [Kapitel Aktivierungsprozess](#). Neben den zu beobachtenden Quellen können dort auch spezifische Fokusse sowie Arbeitsaufgaben definiert werden. Typische Arbeitsaufgaben sind (erweiterte Aufzählung nach Fathi, 2022):

- Digitale Erkundung
  - Informationsbeschaffung, -verarbeitung und -visualisierung aus öffentlich zugänglichen Quellen unter Verwendung von Open Source Intelligence (OSINT) Ansätzen (Bohm, 2021)
  - Verifikation und Falsifikation, z. B. Identifikation von Falschinformationen und Gerüchten
- Verarbeitung der Daten

- Transformation von Rohdaten in eine verständliche und nachvollziehbare Information
- Visualisierung und Aufbereitung der Informationen in schnell und intuitiv verständliche Formate sowie Unterstützung bei der Integration in die Entscheidungsfindung
- Kartierung der relevanten Daten
  - Erstellung von digitalen Karten betroffener Gebiete und deren Aufbereitung mit zusätzlichen Informationen (z.~B. Zufahrtswege, überflutete Gebiete)
  - Visualisierung, Geolokalisierung und räumliche Analyse mit Hilfe geografischer Informationssysteme
- Freiwilligenkoordination und Zusammenarbeit
  - Schnittstelle zu anderen nationalen und internationalen Teams
  - Schaffung eines technischen und kollaborativen Rahmens, der die Zusammenarbeit ermöglicht

Während des aktivierten Zustandes müssen VOST identifizierte Daten, Bild- und Videomaterial sowie einsatzverlauf-spezifische Informationen dokumentieren und sichern, siehe auch [Kapitel Dokumentation](#). Für die Entscheidungsträger:innen werden die Daten zu Informationen aufarbeitet und gebündelt visualisiert, um die Erkundung in der Lage zu ergänzen, siehe [Kapitel Dokumentation](#).

## Teammitglieder

Da die visualisierten Informationen das Ergebnis der Verarbeitung von Daten durch Algorithmen, Analysen und Interpretationen sind, ist eine Vertrauenswürdigkeit der eingesetzten Kräfte essenziell. Darüber hinaus müssen die Teammitglieder in der Lage sein, die Relevanz und Kritikalität von Daten SoMe zu bewerten, wodurch ein grundlegendes Verständnis von Bevölkerungsschutz, Katastrophenhilfe sowie Gefahrenabwehr und Stabsarbeit notwendig wird, sowie spezifisches Wissen über den Einsatz- sowie Lageverlauf. Resultierend werden Anforderungen an den Hintergrund, den Aufnahmeprozess sowie das Know-How der mitarbeitenden Personen in VOST gestellt.

## Abgrenzung zu Digital-Freiwilligen

Ein wesentlicher Unterschied zwischen Mitgliedern von VOST und Digital-Freiwilligen ist die Vertrauenswürdigkeit durch eine bereits vor dem Eintreten einer Einsatzlage entstandene Verbindung mit Katastrophenschutzbehörden (St. Denis, 2012). Während Digital-Freiwillige sich meist eigenständig, spontan und unkoordiniert aufgrund einer KuK in den Einsatz bringen und öffentlich verfügbare Quellen sichten sowie zu Informationsprodukten aufbereiten, haben vertrauenswürdige Digital-Freiwillige („trusted agents“) bereits positiven Kontakt zu Katastrophenschutzbehörden in einer vergangenen Einsatzlage aufgebaut. Beide organisieren sich teilweise in sogenannten V&TCs, mit der Zielsetzung einer koordinierten Tätigkeit und gemeinsamer Zielausrichtung. Dabei kann in vier verschiedene Typen unterschieden werden (Van Gorp, 2014; Fathi, 2020):

- Gemeinschaften, die Softwareplattformen entwickeln,
- Kooperationen im Bereich der Kartierung,
- Netzwerke von verschiedenen Experten, z.~B. kollaborative Technologieentwicklung und
- Gemeinschaften zur Datenerhebung und -analyse.

Allen gemein ist die Konzentration auf Hilfe für die betroffene Bevölkerung. VOST stellen, als eine Gruppierung dezentral tätiger Digital-Freiwilliger zur Datenerhebung, -analyse und -kartierung in besonderen Einsatzlagen, eine besondere Form von V&TCs dar. Diese Teams sind in die etablierten Strukturen von Organisationen und Einrichtungen des Bevölkerungsschutz integrierbar und erfüllen

spezielle Anforderungen an die Mitglieder durch Aufnahmeprozesse (spontane Teilnahme wird dadurch eingeschränkt) (Fathi, 2020).

## Aufnahmeprozess

Der Aufnahmeprozess für Mitglieder in ein VOST ist entscheidend für die Effektivität und das reibungslose Funktionieren des Teams. Es gewährleistet, dass jedes Mitglied über die notwendigen Fähigkeiten, Qualifikationen und das Verständnis verfügt, um in KuK effektiv zu agieren und die gestellten Aufgaben zu erfüllen.

**Vorstellungsgespräch** Potenzielle Mitglieder durchlaufen in der Regel ein Vorstellungsgespräch, um ihre Motivation, Erfahrungen und Fähigkeiten zu bewerten. Dies bietet auch die Gelegenheit, den potenziellen Beitrag des Bewerbers zum Team zu erörtern und sicherzustellen, dass er mit den Zielen und Arbeitsweisen des VOST kompatibel ist

**Prüfung der notwendigen Fähigkeiten und Qualifikationen** Die Überprüfung der Fähigkeiten und Qualifikationen der Bewerber:innen ist ein wichtiger Schritt im Aufnahmeprozess. Dies kann die Beurteilung technischer Fähigkeiten, Kenntnisse im Bevölkerungsschutz, Erfahrungen in den SoMe sowie andere relevante Kompetenzen umfassen.

**Onboarding** Nach erfolgreicher Auswahl durchlaufen neue Mitglieder in der Regel ein Onboarding-Programm, das sie auf ihre Rolle im VOST vorbereitet. Dieses Programm kann interne und externe Prozesse beinhalten, darunter bspw. Einweisungen, Schulungen und Übersicht über interne Prozessdokumentationen.

02\_Voraussetzungen/fig\_prozessdoku.pdf

Das Onboarding kann im inaktivierten wie im aktivierten Zustand erfolgen, sodass ein langsamer Integrationsprozess umgesetzt werden kann. Vor allem für den Anfang der Einführung in die aktivierte Phase bietet sich ein Mentoring an, bei welchem jedem neuen Mitglied ein erfahrenes Mitglied für die direkte Kontaktaufnahme an die digitale Seite gestellt wird. Dadurch kann die Hürde, Fragen zu stellen, verringert werden, da nicht direkt vor dem ganzen Team im gemeinsamen Call agiert werden muss. Nicht zuletzt weil die Tätigkeiten in einem VOST meist ehrenamtlich absolviert werden, ist es wichtig, den neuen Mitgliedern Unterstützung, Motivation und Rat zur Verfügung zu stellen. Darüber hinaus kann die Mentorin oder der Mentor bei der individuellen Zielsetzung sowie Richtungs- und Spezialisierungsfindung beraten. Das Onboarding stellt insgesamt sicher, dass neue Mitglieder des VOST mit den erforderlichen Kenntnissen, Fähigkeiten und Ressourcen ausgestattet sind, um effektiv zur Krisenreaktion und -bewältigung beizutragen. Es fördert außerdem die Integration neuer Mitglieder in das Team und stärkt die Zusammenarbeit und Kommunikation unter den Teammitgliedern.

## Notwendiges Know-How

Die erforderlichen Kenntnisse sind abhängig von der spezifischen Ausrichtung und dem Leistungsportfolio des jeweiligen VOST. Insgesamt können jedoch folgende Punkte in mehreren VOST identifiziert werden:

- Kenntnisse über Tools für Videokonferenzen (bspw. Webex) und digitale Verknüpfung des Teams (bspw. Threema) (aufgrund der dezentralen Tätigkeit ist das Wissen über die digitale Verknüpfung, die Vertrautheit mit den verwendeten Tools sowie die Austauschprozesse im inaktivierten und aktivierten Zustand extrem wichtig)
- Kenntnisse über die interne und externe Kommunikationsstrategie (bspw. welche Kanäle werden für welche Kommunikationsthemen verwendet und erfolgt eine externe Kommunikation in aktivierten/inaktivierten Phasen?)
- Wissen über die prozessuale Struktur im inaktivierten Zustand
- Integration in die Teamstruktur und Bekanntheit der weiteren Teammitglieder (durch die ausschließlich digitale Zusammenarbeit ist dieser Punkt sehr relevant, um eine abgestimmte und zielgerichtete Teamarbeit zu ermöglichen)
- Kenntnisse über die Vorgehensweise und Methodik bei der Einsatztätigkeit im aktivierten Zustand
- Wissen über die Strukturen, Hierarchien und formalen Kommunikationskanäle der Organisation/Struktur, in welche das VOST integriert ist (bspw. Grundlehrgang Bundesanstalt Technisches Hilfswerk)
- Schulungsgrundlagen zu Best Practices, Standards und vergangenen Einsatzgeschehen
- Absolvierung relevanter Online-Kurse (bspw. [Lernkompass des Instituts der Feuerwehr Nordrhein-Westfalens zu Stabsarbeit](#))

Die einzelnen Punkte (notwendige Schulungen, Pflicht- und hilfreiche Lektüre, Einweisungen, etc.) müssen durch jedes VOST individuell festgelegt und im optimalen Fall dokumentiert sowie durch benannte Verantwortliche umgesetzt werden. VOST kennzeichnen sich vor allem durch die Heterogenität der Mitglieder aus. Folglich ist nicht das Ziel, dass alle Mitglieder die gleichen Kenntnisse haben, sondern auf Grundlage einer gemeinsamen Basis eine gegenseitige Vermittlung von technischen Fähigkeiten und Wissen über SoMe sowie Bevölkerungsschutz teilen zu können (St. Denis, 2012).

## Interne Netzwerkorganisation

Die effektive intraorganisationale Netzwerkverknüpfung eines VOST ist von entscheidender Bedeutung für eine koordinierte und reaktionsfähige Krisenbewältigung. Durch eine klare hierarchische Struktur, gut durchdachte Briefingprozesse und angemessene Rahmenbedingungen kann ein VOST effektiv arbeiten und zur Bewältigung von Einsatzlagen beitragen.

02\_Voraussetzungen/fig\_hierarchy.pdf}

Hierarchische Struktur eines VOST (aktualisierte Version von Fathi, 2020)

**Hierarchische Struktur eines VOST** Um möglichst kompatibel mit Entscheidungsträger:innen zu sein, implementiert ein VOST eine hierarchische Struktur, die eine klare Linie der Kommunikation und Entscheidungsfindung ermöglicht. Hierbei fungieren Verbinder:innen als vor Ort physisch anwesend und der anfordernden Stelle angebundener Sprechkanal zwischen dem VOST und den Entscheidungsträger:innen. Gemeinsam mit der Team-/Einsatzleitung bilden die Verbinder:innen eine Koordinierungseinheit, welche die VOST Mitglieder koordinieren. Die obige Abbildung visualisiert in Anlehnung an die Beschreibung und Darstellung von (Fathi, 2020) die intra- und interorganisationale Verknüpfung von VOST. Dabei bildet die Koordinierungseinheit die Verknüpfung zwischen der anfordernden Stelle, der angebotenen Einsatzorganisation oder staatlichen Einrichtung sowie weiteren digitalen Netzwerken oder VOST. Viele etablierte VOST bestehen aus weniger als zehn Mitgliedern. Gemäß der Erkenntnis von (St. Denis, 2012) arbeiten kleinere Teams (4-9 Mitglieder) effektiver, können intern besser koordiniert werden und sind sich der gemeinsamen Ziele und



& & Weitergabe von umsetzbaren Informationen an und Beratung von Entscheidungsträger:innen, Zusammenarbeit mit anderen digitalen Netzwerken und VOST \\ \\ & \multicolumn{2}{l}{\tabitem Intern:} \\ \\ & & Priorisierung von Informationen, Aufbau einer Teamstruktur: Koordination der Arbeitsabläufe, Definition der Informationsprodukte, Zuweisung von Aufgaben, Rollen und Verantwortlichkeiten \\ \\ \\ \\ \midrule

\multirow{6}{3cm}{Verbinder:in} & \\ \multicolumn{2}{l}{\tabitem Hauptaufgabe:} \\ \\ & & Verbindung zwischen digitalem Team und anfordernder Stelle \\ \\ & \multicolumn{2}{l}{\tabitem Extern:} \\ \\ & & Definition der Vorgehensweise (Aufgabenpriorisierung, Informationsbedarfe, -aufbereitung und -übermittlungsprozesse) mit anfordernder Stelle, fachliche Beratung vor Ort, Verteilung der externen Dokumentationen, Abgleich von Informationen aus \ac{some} mit Informationen aus konventionellen Methoden (z.-B. Field Response) mit anfordernder Stelle \\ \\ & \multicolumn{2}{l}{\tabitem Intern:} \\ \\ & & Beitrag über aktuelle Entwicklung in chronologischer Auflistung in regelmäßigen Abständen/Briefings \\ \\ \midrule

\multirow{6}{3cm}{VOST Mitglieder/ Fachhelfer:innen} & \\ \multicolumn{2}{l}{\tabitem Hauptaufgabe:} \\ \\ & & Social Media Monitoring und Social Listening \\ \\ & \multicolumn{2}{l}{\tabitem Extern:} \\ \\ & & - \\ \\ & \multicolumn{2}{l}{\tabitem Intern:} \\ \\ & & dislozierte, selbstständige Tätigkeit, Abstimmungen mit Leitung, groß angelegte Extraktion, Aggregation und Filterung von Informationen aus verschiedenen öffentlich verfügbaren digitalen Quellen \\ \\ \\ \\ Strukturell betrachtet, kann ein VOST einem One-line-System mit hierarchischen Strukturen und definierten Verantwortlichkeiten folgen, wobei Entscheidungen je nach Zeitfenster entweder zentralisiert (durch die Koodinierungseinheit strategisch ausgerichtete Entscheidungen) oder dezentralisiert (durch die Gruppenleiter:innen taktisch ausgerichtete Entscheidungen) werden, siehe auch Abbildung~\ref{fig:StrukturAnforderungen}. Formalisierung ist ein weiteres Merkmal, das durch die definierte Hierarchie, Kommunikationsprozesse und Anforderungsprofile an VOST-Mitglieder gekennzeichnet ist. Prozessuale Anforderungen beinhalten darüber hinaus interne Prozesse wie Leadership-Konzepte und Definitionen von internen Kommunikationskanälen (innerhalb der Arbeitsgruppen sowie im gesamten Team), sowie Prozesse mit externen Partnern, die die Definition von Kommunikationskanälen (welche, zu welchem Zweck, für welche Informationen, etc.), Informationsverteilung (Arten von Informationen, Zeitkritikalität und Relevanzen, Formate, etc.) und Zielgruppen (bspw. Verteilerkreise) umfassen.

## Technische Vorbereitung und Voraussetzungen

Neben den organisatorischen Vorbereitungen und Voraussetzungen muss auch die technische Arbeitsfähigkeit des Teams durchdacht und sichergestellt werden. Hierzu zählen unter anderem

Hardware, Software und Übersichten über vorhandene und nutzbare Webanwendungen.

## Notwendige Hardware und Ausrüstung

Die notwendige Ausstattung aller Mitglieder eines VOST müssen für jedes Team vor Einsatzbereitschaft identifiziert und bereitgestellt werden. Beispielhaft soll hier eine hilfreiche Ausstattung beschrieben werden, welche auf hohem Niveau die Mitarbeit in einem VOST ermöglichen sollte.

Zur Nutzung von gängigen Programmen der Datenerhebung und -bearbeitung sollte jedes Mitglied einen IT-Arbeitsplatz besitzen. Die notwendige Hardware umfasst dabei einen persönlichen Computer (PC), einen Datenspeicher, ein Headset mit Mikrofon, eine Maus, Tastatur und Bildschirme. Der Datenspeicher kann im optimalen Fall online zugreifbar sein, um identifizierte Daten sicher speichern und kollaborativ verwalten zu können. Darüber hinaus ist aufgrund der Erhebung von öffentlich verfügbaren `\textit{digitalen}` Daten eine Anbindung an vorhandene öffentliche oder nicht öffentliche Netze notwendig, sodass ein Router vorhanden sein muss. Für den Verbinder oder die Verbinderin sollte der Router ein portabler LTE-Router sein, um eine Tätigkeit vor Ort, aber getrennt vom Netzwerk des Stabes zu ermöglichen. Ein Smartphone (inkl. SIM-Karte und Zubehör) ermöglicht den Teammitgliedern zusätzlich teilweise einen vereinfachten Zugriff auf bestimmte Quellen (bspw. über Apps von sozialen Netzwerken andere Suchfunktionen) sowie die Kommunikation über Mobilfunknetze.

## Übersicht über Tools, Algorithmen und Anwendungen

Neben der notwendigen Hardware benötigen VOST Mitglieder auch eine funktionsfähige und einsatzbereite Software um einsatzfähig zu sein.

Hierzu zählen ein Monitoringtool (bspw. Hootsuite, um die Identifikation von Daten zu vereinfachen), ein Kollaborationstool (bspw. WebEx, um einen Austausch mit Videoformat im aktivierten und inaktivierten Zustand des Teams zu ermöglichen), ein Analysetool (bspw. Talkwalker, um die identifizierten Daten zu analysieren) sowie eine Geoinformationssoftware (bspw. ArcGIS, zur Kartierung der relevanten Informationen oder Erstellung eines Dashboards). Darüber hinaus kann eine Datenverschlüsselungssoftware (bspw.

`\href{https://www.veracrypt.fr/en/Downloads.html}` {VeraCrypt}) hilfreich sein, um datenschutzrechtlich oder einsatzbedingt kritische Daten zu sichern.

Alle der aufgeführten Nutzungsintentionen können auch mit kostenlos verfügbaren Softwarelösungen oder Webanwendungen umgesetzt werden. Jede Lösung, für die sich ein VOST entscheidet, sollte jedoch bereits vor dem Einsatz getestet und die Funktionsfähigkeit sowie die Anwendungsfähigkeit durch die VOST Mitglieder bekannt sein.

Im Bereich OSINT und SOCMINT haben sich in den letzten Jahren viele verschiedene Webanwendungen und Tools entwickelt, sodass bereits viele Übersichten über vorhandene Möglichkeiten erstellt wurden. Bspw. Übersichten sind `\href{https://osintgeek.de/tools}` {OSINT Geek (Hyperlink)}, `\href{https://s0cm0nkey.gitbook.io/s0cm0nkeys-security-reference-guide}` {s0cm0nkey Security Reference Guide (Hyperlink)} und `\href{https://osintframework.com/}` {OSINT Framework (Hyperlink)}. Bei reddit werden bereits erste Übersicht über die Übersichtslisten erstellt, bspw.

\href{https://www.reddit.com/r/OSINT/comments/12gd5hb/the\_new\_biggest\_osint\_list\_209\_pages\_wor\_th\_of/?rdt=47498}{hier (Hyperlink)}. Darüber hinaus haben verschiedene Personen startpages erstellt, um Linksammlungen übersichtlich zu gruppieren und öffentlich zur Verfügung zu stellen. Beispiele hierfür sind: \href{https://start.me/p/q6naJo/osint-links}{Übersicht über OSINT Links (Hyperlink)}, \href{https://start.me/p/7kxyy2/osint-tools-curated-by-lorand-bodo}{Übersicht über online Ressourcen, aufgeteilt nach FOSINT, GEOINT, OSINT, SOCMINT und SIGINT (Hyperlink)}, sowie \href{https://start.me/p/4KeEek/vostdashboard}{ein VOST Dashboard (Hyperlink)}. Für eine Erklärung der Abkürzung siehe Kapitel~\ref{sec:glossar}. Das \href{https://i-intelligence.eu/uploads/public-documents/OSINT\_Handbook\_2020.pdf}{Open Source Intelligence Tools and Resources Handbook 2020 (Hyperlink)} führt diverse solcher Listen gruppiert und klassifiziert auf. Auch auf GitHub werden solche Listen geführt und ermöglichen eine Mitwirkung bei der Aktualisierung auf Grundlage dieses Handbuchs, bspw. diese \href{https://github.com/jivoi/awesome-osint}{Übersicht über OSINT Tools und Ressourcen (Hyperlink)}, \href{https://github.com/osintambition/Social-Media-OSINT-Tools-Collection}{Social-Media-OSINT-Tools-Collection (Hyperlink)} und \href{https://github.com/jieyab89/OSINT-Cheat-sheet}{OSINT CHEAT SHEET (Hyperlink)}.

Neben den Listen für Webanwendungen gibt es auch diverse Open Source Anwendungen mit und ohne graphische Nutzeroberfläche, welche bspw. Browsererweiterungen für OSINT (z. B. \href{https://github.com/mitchmoser/sputnik}{Sputnik OSINT Extension (Hyperlink)} und \href{https://github.com/ninoseki/mitaka}{Mitaka (Hyperlink)}), Suchmöglichkeiten (z. B. \href{https://github.com/opsdisk/metagoofil}{Metagoofil (Hyperlink)}), OSINT tools (z. ~B. \href{https://github.com/lanmaster53/recon-ng}{The Recon-ng Framework (Hyperlink)} und \href{https://github.com/laramies/theHarvester}{theHarvester (Hyperlink)}) sowie Geolokalisierungstools (z. B. \href{https://www.geocreepy.com/}{GeoCreepy (Hyperlink)}) umfassen.

Ein VOST kann spezifische Listen/Übersichten für die eigene Arbeit erstellen. Insgesamt profitiert die Effizienz des Teams jedoch auch davon, dass jedes Mitglied eigene Fähigkeiten und Herangehensweisen an die Datenerhebung hat.

## Eigenschutz der Teammitglieder

Der Eigenschutz der Mitglieder eines VOST ist von grundlegender Bedeutung, um sicherzustellen, dass sie effektiv und nachhaltig zur Krisenbewältigung beitragen können. Dieses Kapitel widmet sich der Aufklärung über verschiedene Aspekte des Eigenschutzes. Während VOST-Mitglieder ihre Fähigkeiten und Ressourcen einsetzen, um anderen in besonderen Einsatzlagen zu helfen, ist es unerlässlich, dass sie auch ihre eigene Sicherheit im Auge behalten. Durch ein ganzheitliches Verständnis und die Umsetzung von Eigenschutzmaßnahmen können VOST-Mitglieder ihre Effektivität maximieren und gleichzeitig das Risiko für sich selbst minimieren. Gefährdungen, welche bei einem virtuellen Einsatz auf die Einsatzkräfte und/oder ihre Ausstattung wirken, lassen sich dabei grob in drei Kategorien unterteilen:

1. Gefährdungen für die psychische Gesundheit,
2. die informationelle Selbstbestimmung und
3. die technische Ausstattung der Einsatzkräfte.

Während Schutzfaktoren der informationellen Selbstbestimmung der Einsatzkräfte, also den Schutz privater, sensibler Informationen, sowie der technischen Ausstattung (bspw. vor Schadsoftware) in Kapitel~\ref{subsubsec:technischerEigenschutz} behandelt werden, wird auf den Schutz der psychischen Gesundheit der eingesetzten Kräfte in Kapitel~\ref{subsubsec:psychischerEigenschutz}

eingegangen.

## Technischer Eigenschutz

Grundsätzlich sollten sich Teammitglieder von VOST bei der Arbeit mit elektronischen Geräten darüber bewusst sein, dass immer die Gefahr besteht, mit Schadprogrammen in Kontakt zu kommen. Einen absoluten Schutz hiervoor gibt es nicht. Es gibt jedoch Möglichkeiten, das Risiko einer Infektion der eingesetzten Systeme zu verringern. Durch die Anbindung von VOST an Einsatzorganisationen oder staatliche Einrichtungen, sollten zunächst die in der angebotenen Organisation zuständigen Abteilungen für IT-Sicherheit und Datenschutz die geltenden Rahmenbedingungen übermitteln und erklären.

Grundsätzlich sollten OSINT und SOCMINT nicht auf Geräten durchgeführt werden, welche sich innerhalb kritischer Netzwerke befinden oder deren Ausfall schwerwiegende negative Auswirkungen und Schäden nach sich ziehen könnte. Folglich sollten die durch VOST Mitglieder genutzten Systeme nicht direkt in das Netz der leitenden/anfordernden Stelle integriert sein. Darüber hinaus sollten im Team Möglichkeiten wie bspw. eine virtuelle Maschine (z. B. VirtualBox oder VMware) genutzt werden. Virtuelle Maschinen kapseln ein Rechnersystem software-technisch innerhalb eines lauffähigen Rechnersystems ab. Dadurch wird eine Rechnerarchitektur eines real in Hardware existierenden Rechners nachgebildet.

Für die Tätigkeiten als VOST Mitglied werden folgende Punkte empfohlen (bsph. für ein Windows-System \cite{Windows}):

- Aktualisieren Sie Ihr Betriebssystem und Ihre Software regelmäßig: Stellen Sie sicher, dass Windows und alle installierten Programme auf dem neuesten Stand sind, um bekannte Sicherheitslücken zu schließen.
- Verwenden Sie eine zuverlässige Antivirensoftware: Installieren Sie eine vertrauenswürdige Antivirensoftware und halten Sie sie stets aktiv und auf dem neuesten Stand, um potenzielle Bedrohungen frühzeitig zu erkennen und zu blockieren.
- Aktivieren Sie die Firewall: Schalten Sie die integrierte Windows-Firewall ein, um unerwünschten Netzwerkzugriff zu blockieren und Ihre Privatsphäre zu schützen.
- Seien Sie vorsichtig beim Herunterladen von Dateien: Laden Sie Dateien nur von vertrauenswürdigen Quellen herunter und vermeiden Sie verdächtige Links oder Anhänge in E-Mails oder auf Webseiten.
- Überprüfen Sie regelmäßig Ihre Sicherheitseinstellungen: Nehmen Sie sich Zeit, um Ihre Sicherheitseinstellungen auf Ihrem PC zu überprüfen und anzupassen, um unerwünschte Zugriffe zu verhindern und Ihre Privatsphäre zu schützen.
- Verwenden Sie starke Passwörter: Verwenden Sie komplexe Passwörter für Ihre Konten und ändern Sie sie regelmäßig, um sicherzustellen, dass Ihre persönlichen Daten geschützt sind.
- Sichern Sie regelmäßig Ihre Daten: Führen Sie regelmäßige Backups Ihrer wichtigen Dateien durch, um sich vor Datenverlust durch Ransomware oder andere Bedrohungen zu schützen.
- Seien Sie vorsichtig bei der Verwendung von öffentlichem WLAN: Vermeiden Sie die Übertragung sensibler Informationen über öffentliche WLAN-Netzwerke und verwenden Sie wenn möglich ein virtuelles privates Netzwerk (VPN), um Ihre Verbindung zu verschlüsseln und Ihre Daten zu schützen.

Allgemeine Informationen zum sicheren Umgang mit IT-Geräten finden Sie auch auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (vgl.

\cite{BSI\_Verbraucherinfo.2023}) und auf der \href{https://digitalcourage.de/digitale-selbstverteidigung}{Seite des gemeinnützigen Vereins Digitalcourage}. Bei Fragen zum Thema Cybersecurity können sich behördliche Organisationen auch an das BSI wenden und von diesem beraten lassen.

Aufgrund der besonderen Einsatzfähigkeiten von VOST werden folgend mögliche Maßnahmen zur Prüfung von unbekanntem Webseiten, unbekanntem oder verdächtigen Dateien sowie zum Schutz persönlicher Dateien angerissen. Jedes Team sollte sich jedoch über die eigene Risikoakzeptanz und daraus resultierende notwendige Schutzmaßnahmen Gedanken machen.

## Unbekannte Webseiten prüfen

Sind Sie sich unsicher, ob Sie einer Ihnen unbekanntem Internetseite trauen können, oder ob sich hinter dieser eventuell schadhafte Inhalte verbergen, können Sie die betreffende Adresse mit dem kostenlosen Online-Tool \href{https://www.virustotal.com/gui/home/url}{VirusTotal} prüfen. Geben Sie dazu in dem Feld \textit{Search or Scan a URL} die von Ihnen gewünschte Adresse ein und bestätigen Sie die Eingabe mit der \textit{Enter}-Taste. Im Anschluss erhalten Sie eine Übersicht darüber, wie die Adresse durch die von VirusTotal abgefragten Cyber-Security-Produkte eingeschätzt wird (vgl. Abbildung \ref{fig:21\_virustotal\_url\_check}).

02\_Voraussetzungen/virustotal\_url\_scan.png

Screenshot: Ergebnis eines URL-Scans bei \href{https://www.virustotal.com}{VirusTotal} für die Domäne der Universität Wuppertal

## Unbekannte oder verdächtige Dateien prüfen

Seien Sie sich bei der Arbeit mit einem Computer darüber bewusst, dass es vielfältige Angriffsmechanismen gibt, welche durch Angreifer genutzt werden. Schadprogramme müssen nicht zwingend als Anwendung, unter Windows beispielsweise als .exe-Datei, auf ihr System gelangen. Auch PDF-, Multimedia- oder Office-Dateien können schadhafte Code enthalten oder Schadprogramme ohne Ihr Wissen im Hintergrund herunterladen und ausführen. Auch die Verwendung eines Antivirensystems bringt hier keine absolute Sicherheit, da diese Systeme nicht jedes Schadprogramm als solches erkennen beziehungsweise bereits minimale Änderungen am Schadcode ausreichen, um die Signatur der Datei ausreichend zu ändern, sodass diese nicht mehr mit einer eventuell in einer Antivirendatenbank enthaltenen Prüfsumme übereinstimmt. Sicherer ist es da bereits, wenn Sie mehrere Datenbanken abfragen. Hierzu bietet die Plattform \href{https://www.virustotal.com}{VirusTotal} die Möglichkeit, verdächtige Dateien hochzuladen und die Signatur mit bis zu 90 verschiedenen Datenbanken aus dem Bereich der Cyber-Security abzugleichen. Um dies zu nutzen, gehen Sie bei \href{https://www.virustotal.com}{VirusTotal} auf \textit{Choose file}. Wählen Sie anschließend die Ihnen unbekanntem Datei aus und bestätigen Sie nach dem Hochladen der Datei mit einem Klick auf die Schaltfläche \textit{Confirm upload}. Anschließend wird die Datei analysiert und Ihnen wird ein Ergebnis ähnlich zu dem in Abbildung \ref{fig:21\_virustotal\_url\_check} dargestellten Ergebnis angezeigt.

**Wichtig ist, dass Sie die Analyse vor dem ersten Öffnen der Datei auf Ihrem System durchführen. Sollten Sie eine Datei zuvor bereits geöffnet haben und der Scan positiv ausgefallen sein, so sollten Sie Ihr System als infiziert betrachten und umgehend Ihren IT-**

**Systemadministrator kontaktieren. Trennen Sie in diesem Fall umgehend das System vom Netzwerk, um eine Ausbreitung möglichst zu verhindern.**

## Schutz persönlicher Informationen

Achten Sie darauf, ihre persönlichen Informationen zu schützen. Vermeiden Sie es bestmöglich, private Nutzungszugänge und Accounts in \ac{some} für Ihre VOST Tätigkeit zu nutzen. Nur auf diese Weise ist es möglich, sicherzustellen, dass sie weder absichtlich, noch unabsichtlich private Informationen über sich und Verwandte preisgeben. Accounts, welche durch das VOST genutzt werden, sollten idealerweise im Rahmen der Einsatzvorbereitung bereits angelegt und regelmäßig gepflegt werden.

## Psychischer Eigenschutz

Die psychische Gesundheit der Einsatzkräfte leistet einen wesentlichen Beitrag zum Einsatzerfolg – das gilt auch für VOST. Dementsprechend sind Maßnahmen zu ergreifen, die psychische Belastungen im Einsatz reduzieren. Dabei müssen vor allem die Rahmenbedingungen, unter denen Einsätze abgearbeitet werden, in den Blick genommen werden, denn nur ein Teil der Belastung erwächst unmittelbar aus dem eigentlichen Einsatzgeschehen.

Ob ein Einsatz zu einer Belastung der Einsatzkraft führt, kann nicht pauschal beurteilt werden, denn hierauf haben individuelle Faktoren wesentlichen Einfluss. Dies sind die persönlichen Voraussetzungen der Einsatzkraft, die Risiken, die ein konkreter Einsatz mit sich bringt, und die Risiken, die sich aus dem Umgang der Einsatzkraft mit einem Einsatzgeschehen ergeben.

Zu den persönlichen Voraussetzungen zählen beispielsweise Ausbildungsstand und Einsatzerfahrungen, Lebensstil (z. B. Ernährung, Bewegung) oder die aktuelle Lebenssituation. Eine sachliche und die eigenen Grenzen respektierende Einschätzung der eigenen Verfassung ist vor Einsatzbeginn daher Aufgabe jeder Einsatzkraft. Risiken aus dem Einsatzgeschehen ergeben sich aus der Konfrontation mit Daten aus dem Einsatzgebiet. Insbesondere sind dies Text-, Bild- und Tondokumente. Möglicherweise kann aber auch der Einsatzverlauf zur Belastungsquelle werden, wenn beispielsweise technische oder kommunikative Probleme den Einsatzerfolg gefährden. Zu den Risiken aus dem Umgang mit einem Einsatzgeschehen zählt beispielsweise die Überschätzung der eigenen Belastbarkeit. „Gerade für VOST-Kräfte erscheint dieses Risiko erhöht, da sie alleine am Rechner agieren und die Beobachtung SoMe eine Aufgabe darstellt, die faktisch keinen natürlichen Endzeitpunkt kennt. Wird ein Einsatz daher nicht bewusst unterbrochen oder beendet, so ist es denkbar, dass Pausenzeiten, Ernährung, Bewegung und andere notwendige Aktivitäten, die die Selbstsorge betreffen, dem Einsatzziel untergeordnet werden und damit die Anfälligkeit für psychische Belastungen steigt.“ (Tutt, 2022) Die Verantwortung für die psychische Gesundheit liegt bei allen Einsatzkräften, die ihre Einsatzfähigkeit beurteilen und auf ihren Selbstschutz achten müssen. In der Verantwortung stehen aber auch Führungskräfte. Diese sind für die Einsatzvorbereitung, Einsatzkräfteausbildung und die Einsatzplanung verantwortlich und haben damit erheblichen Einfluss auf die Begrenzung von Belastungen. Dabei ist ein besonderes Augenmerk auf die Entwicklung der gemonitornten SoMe-Kanäle zu legen. Ein Facebook-Kanal kann zum Einsatzbeginn

noch 150 Aktivist:innen und innerhalb kürzester Zeit mehrere tausend vorweisen, sodass hier eine Überforderung durch die Datenmasse entstehen kann. Insgesamt sind die Rahmenbedingungen eines Einsatzes von hoher Bedeutung für das Ausmaß möglicher Belastung.

**Psychosoziale Notfallversorgung für Einsatzkräfte** Die Psychosoziale Notfallversorgung für Einsatzkräfte (PSNV-E) erkennt dies an, indem sie der primären Prävention – also der Vorsorge im Einsatzvorfeld – breiten Raum gibt. Dementsprechend ist die PSNV-E ein mehrgliedriges System, welches unterschiedliche Ressourcen einbindet, um die Einsatzfähigkeit und den Gesundheitsschutz der Einsatzkräfte sicherzustellen. Neben der primären Prävention umfasst sie die Einsatzbegleitung und die Nachbereitung durch spezifisch geschultes Personal (sekundäre Prävention) sowie die Überführung in langfristige Hilfen mit den Ziel der Vermeidung dauerhafter Beeinträchtigung (tertiäre Prävention). In dieser letzten Phase können sehr unterschiedliche Ressourcen zum Einsatz kommen. Diese reichen vom stabilisierenden familiären Umfeld bis zur medizinisch-therapeutischen Begleitung und hängen von der Art der Belastung und von der Bewältigungsfähigkeit der betroffenen Einsatzkraft ab. Abbildung~\ref{fig:psnv-e} verdeutlicht den Aufbau der PSNV-E.

Wie andere Einsatzkräfte sind auch VOST-Kräfte besonderen Belastungen ausgesetzt. Die Distanz zum Ereignisort, die bei virtuell arbeitenden Helfer:innen vielfach gegeben ist, darf hierbei nicht als Schutz missverstanden werden. Vielmehr ergeben sich aus der besonderen Einsatzsituation veränderte Belastungsquellen. Nicht selten würden Helfer:innen gerne unmittelbar vor Ort in das Einsatzgeschehen eingreifen, statt den Einsatz virtuell zu begleiten. In einer nicht-repräsentativen Umfrage unter Einsatzkräften aus acht VOST im Rahmen eines #sosmap-Workshops stimmten 77~Prozent der Antwortgebenden der Aussage „Manchmal wäre ich gerne vor Ort gewesen, um unmittelbar helfen zu können.“ tendenziell zu. Die fehlende Möglichkeit unmittelbar zu wirken, bei gleichzeitig vergleichsweise gutem Bild der Einsatzlage, ist eine potenzielle Belastungsquelle, wenn die Situation mit einem Gefühl von Machtlosigkeit empfunden wird. Ein weiterer Belastungsfaktor, der sich in diesem Zusammenhang in VOST-Einsätzen gezeigt hat, ist „Frustration über Lagebewältigung vor Ort“.

02\_Voraussetzungen/fig\_psychEigenschutz.pdf

Mehrgliedrigkeit der Psychosozialen Notfallversorgung für Einsatzkräfte (PSNV-E) (in Anlehnung an \cite{BBK.2012})

Hiermit im Zusammenhang steht, dass VOST-Einsatzkräften häufig dauerhaft eine Vielzahl von Dokumenten aus der Frühphase (Chaosphase) einer Lage begegnet und daher der subjektive Eindruck der Lagebewältigung verzerrt sein kann. Zudem liegt es in der Logik SoMe, dass besonders gravierende Aspekte einer Lage vielfach verbreitet werden und daher VOST-Einsatzkräften die Relativierung durch andere, neutralere Eindrücke schwerer möglich ist.

Ein weiterer VOST-spezifischer Belastungsfaktor ist die begrenzte Möglichkeit zum Stressabbau aufgrund der geringen körperlichen Aktivität im Einsatz vor dem Rechner. Dem kann durch verbindliche Pausenregelungen und Ausgleich-Aktivitäten entgegengewirkt werden. An die Stelle von Ruhezeiten sollten hier bewusste körperliche Aktivierungsphasen treten. Weitere mögliche Belastungsfaktoren unterscheiden sich dagegen kaum von denen anderer Einsatzkräfte. Hierzu zählen beispielsweise Zeitdruck oder Mitleid mit Betroffenen.

**Belastungsreaktionen** Zeigen Einsatzkräfte Belastungsreaktionen, so ist dies zunächst ein gesundes Verhalten eines gesunden Organismus im Umgang mit einer außergewöhnlichen Situation. Keineswegs müssen solche Reaktionen als Anzeichen für eine mögliche Erkrankung gedeutet werden.

Sie stellen zunächst eine normale Reaktion auf ein außergewöhnliches Ereignis dar und lassen sich in körperliche, kognitive, emotionale und soziale Reaktionen einteilen. Die Bandbreite der Reaktionen ist groß und individuell höchst verschieden. Insofern ist es auch nicht sinnvoll, eigene Reaktionen mit denen anderer Einsatzkräfte zu vergleichen.

Die nachfolgende Auflistung ist eine unvollständige Zusammenstellung, die lediglich Breite des Reaktionsspektrums verdeutlichen soll:

- Schlafstörungen
- Rast-/ Ruhelosigkeit
- erhöhter Puls/Blutdruck
- Müdigkeit
- Übelkeit
- Hunger
- Appetitlosigkeit
- Verdauungsstörungen
- Zähneknirschen
- Verwirrung
- Entscheidungsprobleme
- Desorientierung
- Misstrauen
- Alpträume
- Konzentrationsschwäche
- Erinnerungslücken
- Angst
- Schuldgefühle
- erhöhte Erregbarkeit
- Gefühlsausbrüche
- Gefühlsarmut
- Zurückgezogenheit
- Überempfindlichkeit

Veränderungen lassen sich idealerweise im Vergleich von körperlicher, geistiger und emotionaler Verfassung sowie im (Sozial-)Verhalten vor und nach einem Einsatz feststellen. Hier liegt eine besondere Herausforderung für VOST-Kräfte, die vielfach separiert voneinander am Computer tätig werden und daher weniger Möglichkeit der Beobachtung von Veränderungen bei ihren Teammitgliedern haben. Insofern kommt dem sozialen Umfeld von VOST-Einsatzkräften eine besondere Rolle in der Beurteilung zu. Im Einsatzvorfeld ist es daher sinnvoll, Freunde und Familie für die „Beobachtende Rolle“ zu sensibilisieren.

**Prävention in verschiedenen Einsatzstadien** Der Schutz vor belastungsbedingten Beeinträchtigungen beginnt nicht erst mit dem Einsatz, sondern bereits in der Ausbildung von Einsatzkräften. Das Wissen um mögliche Belastungen und Belastungsreaktionen ist wesentliche Voraussetzung, um im Bedarfsfall angemessen mit diesen Reaktionen umgehen zu können und um Reaktionen richtig zu deuten. Auch ermöglicht die präventive Auseinandersetzung mit psychischen Einsatzrisiken das Erkennen individueller Risikofaktoren und biografischer Vorbelastungen. Zudem wirkt das Wissen um psychosoziale Unterstützung auch dann entlastend, wenn diese Unterstützung nicht in Anspruch genommen wird \cite{Krusemann, 2006}.

Im Einsatz kann präventiv gehandelt werden, indem der eigene Einsatz nicht nur entsprechend der

Bedarfe sondern entsprechend der Fähigkeiten, der eigenen Lebenssituation und der (gesundheitlichen) Verfassung gestaltet wird. Dies kann bedeuten, dass VOST-Kräfte, die aufgrund der genannten Aspekte potenziell verwundbarer erscheinen, etwa weil sie weniger Möglichkeiten haben, mit auftretender Belastung umzugehen als andere, stärker organisatorische oder technische Aufgaben (beispielsweise im Bereich der Kartierung von Lageinformationen) wahrnehmen und die Informationsgewinnung und Sichtung anderen Kräften überlassen. Bei belastenden Einsätzen ist eine systematische Einsatzbegleitung und -nachbesprechung angezeigt. Diese sollte durch Einsatzkräfte erfolgen, die sowohl im Bereich des VOST als auch im Bereich der PSNV über entsprechende Qualifikation und Erfahrung verfügen und „auf Augenhöhe“ mit den Einsatzkräften sprechen können (Peers). Wichtig ist hierbei, dass die in Einsatzbegleitung und -nachbereitung eingesetzten Peers nicht als Einsatzkräfte an dem belastenden Einsatz teilgenommen haben. Nur so ist eine professionelle Distanz zu gewährleisten.

In der Praxis hat sich bei länger andauernden VOST-Einsätzen bewährt, dass an jedem Einsatztag zur immer gleichen Uhrzeit eine bewusste Einsatzunterbrechung erfolgt, die der PSNV dient. Hier wird über den Umgang mit möglichen Belastungen im Sinne einer Sensibilisierung und Psychoedukation gesprochen. Im Rahmen einer solchen „virtuellen Unterbrechung“ ist allerdings dringend davon abzuraten, konkrete belastende Situationen zu besprechen, da ein individuelles Betreuen von betroffenen Einsatzkräften aus der Distanz schwer umsetzbar erscheint. Vielmehr sollte die Unterbrechung genutzt werden, um auf weiterführende Hilfen und Ansprechpartner hinzuweisen. Nach Einsatzende sind Einsatznachbesprechungen im Sinne einer Demobilisierung auch im virtuellen Raum umsetzbar. Auch hierfür gilt, dass konkrete Belastungen kein Thema sein sollten. Demgegenüber gilt es Fakten zum Einsatzverlauf zu vermitteln, um eventuelle Informationslücken zu schließen und damit den Raum für „Kopfkino“ gering zu halten. Zudem sollte auch hier der Verweis auf weiterführende PSNV-Angebote erfolgen.

Grundsätzlich gilt, dass nach psychisch herausfordernden Einsätzen all das gut tut, was auch sonst zum Wohlbefinden beiträgt. Den individuellen Vorlieben entsprechend sind die Möglichkeiten dabei vielfältig. Von Sport bis zu gutem Essen, Musikhören oder einem Spaziergang ist alles denkbar. Untersuchungen haben gezeigt, dass nach belastenden Ereignissen einige Faktoren in besonderer Weise stabilisierend wirken. Das Erleben von Sicherheit, Beruhigung, Selbstwirksamkeit, Kontakt und Anbindung sowie das Fördern von Hoffnung gehören dazu. Dies können sich auch VOST-Kräfte zunutze machen. Bereits im Einsatzvorfeld ist es sinnvoll, sich Gedanken darüber zu machen, was dem eigenen Sicherheitsgefühl zuträglich ist. Dies können reale Orte oder virtuelle Schutzmechanismen sein. Auch die Frage, was zur Beruhigung und Entspannung beiträgt kann vor Beginn des Einsatzes durchdacht werden. Ein Blick auf die Selbstwirksamkeit kann im Rahmen der erwähnten „virtuellen Unterbrechung“ oder des Debriefings erfolgen. VOST-Führungskräfte sollten dabei besonders hervorheben, in welcher Weise anfordernde Stellen die durch VOST generierten Informationen zur Lagebewältigung nutzen konnten. Der von Hobfoll zuletzt genannte Punkt des Förderns von Hoffnung kann sowohl individuell als auch im Team umgesetzt werden. Auf individueller Ebene stehen dabei eigenen positive Bewältigungserfahrungen oder die eigene Religiosität im Vordergrund. Bei der Bewältigung im Team können dies „Hoffnungsgeschichten“ sein, die im Rahmen der Lageerkundung und des Monitorings gesichtet wurden und die mit dem Team geteilt werden.

[Zurück zum vorherigen Kapitel](#)[Zurück zur Übersicht: VOST-Methodenhandbuch](#)[Weiter zum nächsten Kapitel](#)

Last update: 2025/01/08 14:34  
vost-methodenhandbuch:vorbereitung <https://wiki.uni-wuppertal.de/!sosmap/doku.php?id=vost-methodenhandbuch:vorbereitung&rev=1736343283>

From:  
<https://wiki.uni-wuppertal.de/!sosmap/> - **sosmap**

Permanent link:  
<https://wiki.uni-wuppertal.de/!sosmap/doku.php?id=vost-methodenhandbuch:vorbereitung&rev=1736343283>

Last update: **2025/01/08 14:34**

