Ilona Biernacka-Ligięza

Dariusz Dymek

Konrad Glejt

Damian Flisak

Adam Jaskulski

Mikołaj Tomaszyk

Łukasz Żyszkiewicz

Cross-AI Connect: Strengthening Border Resilience

- Projektbericht -

Słubice – Frankfurt (Oder) – Poznań 2025

Redakteure:

dr hab. Agnieszka Bielawska, UAM

prof. UAM dr hab. Mikołaj Tomaszyk, UAM

Herausgeber:

Wydawnictwo Naukowe Wydziału Nauk Politycznych i Dziennikarstwa

ul. Uniwersytetu Poznańskiego 5
61-614 Poznań

Polska

Kontakt zu den Verfassern:

wydawnictwownpid@amu.edu.pl

ISBN 978-83-68190-55-7

eISBN 978-83-68190-56-4

INHALTSVERZEICHNIS

Sylwia COR, Marcin KRZYMUSKI 1
EINFÜHRUNG 1
Mikołaj TOMASZYK 2
KAPITEL I. WIDERSTANDSFÄHIGKEIT (RESILIENZ) UND KRISENMANAGEMENT – ALLGEMEINE ANMERKUNGEN 2
Konrad GLEJT 16
KAPITEL II. KÜNSTLICHE INTELLIGENZ ALS UNTERSTÜTZUNG FÜR KRISENKOMMUNIKATIONSSYSTEME 16
Ilona BIERNACKA-LIGIĘZA 26
KAPITEL III. KOMMUNIKATION AN DER GRENZE DER KULTUREN IM ZEITALTER DER DIGITALEN GLOBALISIERUNG 26
Damian FLISAK 41
KAPITEL IV. NATIONALE UND EUROPÄISCHE RECHTSRAHMEN IM BEREICH CYBERSICHERHEIT UND KI-INSTRUMENTE 41
Adam JASKULSKI 50
KAPITEL V. ETHISCHE UND DATENSCHUTZRELEVANTE ASPEKTE DER NUTZUNG KÜNSTLICHER INTELLIGENZ IM KRISENMANAGEMENT 50
Dariusz DYMEK 61
KAPITEL VI. ORGANISATORISCHE VERÄNDERUNGEN IM BEREICH DES KRISENMANAGEMENTS IN POLEN 61
Dariusz DYMEK, Mikołaj TOMASZYK, Łukasz ŻYSZKIEWICZ 67
KAPITEL VII. KRISENMANAGEMENT IN GRENZÜBERSCHREITENDEN REGIONEN – ALLGEMEINE BEMERKUNGEN 67
Mikołaj TOMASZYK 76
KAPITEL VIII. DETAILLIERTE FORSCHUNGSERGEBNISSE 76
EMPFEHLUNGEN 92
ZUSAMMENFASSUNG 97
LITERATURVERZEICHNIS 99
VERZEICHNIS DER ABBILDUNGEN, TABELLEN UND DIAGRAMME 104
BIOGRAMME 105

Sylwia COR, Marcin KRZYMUSKI

EINFÜHRUNG

Dieser Bericht wurde im Rahmen des Projekts „Cross-AI Connect: Strengthening Border Resilience (CAIR)" erstellt, das dank der Unterstützung des Programms „Resilient Borders" realisiert wurde, welches von der Europäischen Kommission im Rahmen des Pilotprojekts des Europäischen Parlaments „Cross/Border Crisis Response Integrated Initiative'(CB-CRII)" [1] finanziert wird. Dieses Programm spielt eine Schlüsselrolle bei der Stärkung der Widerstandsfähigkeit von Grenzregionen durch die Entwicklung der Zusammenarbeit in den Bereichen Raumplanung und Krisenmanagement. Dank des Fördermittelgebes war es möglich, Pilotmaßnahmen durchzuführen, deren Ergebnisse nicht nur lokale, sondern auch europäische Bedeutung haben.

Das CAIR-Projekt, das in der deutsch-polnischen Doppelstadt Słubice – Frankfurt (Oder) durchgeführt wurde, hat bewiesen, dass moderne Technologien – einschließlich Lösungen auf der Basis künstlicher Intelligenz – die Effektivität des Krisenmanagements signifikant unterstützen können. Im Zuge der Arbeiten gelang es:

- die wichtigsten Bedürfnisse und Barrieren der grenzüberschreitenden Zusammenarbeit im Bereich des Krisenmanagements zu identifizieren,
- das Potenzial digitaler Werkzeuge für die Krisenkommunikation und Übersetzungen zu überprüfen,
- die Akzeptanz und Bereitschaft der Dienste zur Nutzung neuer Technologien zu untersuchen und
- rechtliche, organisatorische und technische Empfehlungen für den Einsatz moderner Lösungen zu erarbeiten.

Diese Ergebnisse haben eine praktische Dimension – sie haben das Potenzial, die Sicherheit und Effizienz der Dienste in der Region zu erhöhen – aber auch eine strategische Dimension, da sie Richtungen aufzeigen, die in anderen Grenzregionen Europas angewendet werden können. Projekt CAIR zeigt, dass grenzüberschreitende Zusammenarbeit, gemeinsame Planung und Investitionen in Innovationen notwendige Voraussetzungen für den Aufbau widerstandsfähiger und integrierter Grenzgemeinschaften sind.

Projektbegünstigte war die Gemeinde Słubice, die das Vorhaben in enger Zusammenarbeit mit der Stadtverwaltung Frankfurt (Oder) umsetzte. Diese grenzüberschreitende Partnerschaft war von entscheidender Bedeutung für den Erfolg des gesamten Prozesses, da sie es ermöglichte, Lösungen unter realen Bedingungen der Arbeit von Diensten und Verwaltung auf beiden Seiten der Grenze zu testen.

Mikołaj TOMASZYK

KAPITEL I. WIDERSTANDSFÄHIGKEIT (RESILIENZ) UND KRISENMANAGEMENT – ALLGEMEINE ANMERKUNGEN

Ein systematischer Ansatz für das Thema Krisenmanagement ist unerlässlich, sowohl aus methodischer Sicht als auch in Bezug auf die Praxeologie und die bisher gewonnenen Erkenntnisse aus der Krisenplanung in dicht besiedelten Gebieten.

Zu diesen Gebieten gehören zweifellos Städte unterschiedlicher Größe und die sich um sie herum entwickelnden funktionalen Gebiete, die aus kleineren Einheiten der Gebietskörperschaften bestehen und gemeinsam einen funktionalen Stadtorganismus bilden. Angesichts der sich in vielerlei Hinsicht dynamisch entwickelnden funktionalen Stadtgebiete (Suburbanisierungsprozess) und im Falle von Doppelstädten der grenzüberschreitenden funktionalen Gebiete, ist es eine Herausforderung, die Verwaltungseinheiten der Dienste, Inspektionen und Feuerwehren entsprechend anzupassen. Die Rolle und Aufgabe der kommunalen öffentlichen Verwaltung in dieser Situation ist die enge Zusammenarbeit, sowohl bei der Identifizierung von Risiken und der Prognose von Bedrohungen als auch bei der Zuweisung von Kräften und Mitteln sowie bei der Durchführung von reaktiven Maßnahmen, die darauf abzielen, den Zustand vor der durch einen Vorfall oder eine Krisensituation verursachten Störung wiederherzustellen.

Hinsichtlich der grenzüberschreitenden funktionalen Gebiete sind diese Herausforderungen noch deutlich vielfältiger. Dazu gehören unter anderem: die Kommunikation in verschiedenen Sprachen, die Koordination von Diensten und Verwaltungen, die in zwei unterschiedlichen Rechts- und Organisationssystemen arbeiten, und andere Aspekte.

Darauf wird in den Schlussfolgerungen aufmerksam gemacht, die nach Abschluss der Operation FENIKS[1] erarbeitet wurden, welche am 23. September 2024 begann und am 30. April 2025 endete. Die Hauptaufgabe dieser Operation war die Unterstützung der Organe der öffentlichen Verwaltung bei der Umsetzung der Aufgaben zur Verhütung und Beseitigung der Folgen von Überschwemmungen und Hochwasser. Die Zusammenarbeit der öffentlichen Verwaltung, der Dienste, Inspektionen und Feuerwehren mit den militärischen Einheiten war von entscheidender Bedeutung. Eine vorrangige Aufgabe war die De-Konfliktualisierung der von verschiedenen Akteuren im Operationsgebiet durchgeführten Aufgaben.[2] Eines der Mittel zur Deeskalation von Konflikten in der Zusammenarbeit verschiedener Akteure ist die Verbesserung des Informationsaustauschs, der Aufbau von Vertrauensmaßnahmen zwischen den Institutionen sowie das aufgebaute Beziehungskapital. Zur

1 Diese Operation wurde im Rahmen der Umsetzung der Aufgaben der separaten Streitkräfte und Mittel der polnischen Streitkräfte zur Bekämpfung und Beseitigung der Folgen der Überschwemmungen durchgeführt.

2 Bericht über die Operation FENIKS, S. 13 (eigene Quelle).

Unterstützung des Informationsaustauschs spielen Kommunikationssysteme und die Nutzung verfügbarer IT-Tools eine wichtige Rolle.

In Ausnahmezuständen wird die Krisenmanagementtätigkeit durch die Visualisierung der Krisensituation, die Aufrechterhaltung der Satellitenkommunikation sowie den Austausch von offenen und geheimen Informationen unterstützt. Während der Operation FENIKS wurden zu diesen Zwecken unter anderem die Satellitensysteme STARLINK, das System POLLYCOM und das Krisenmanagementsystem JAŚMIN, das Funkkommunikationssystem TETRA sowie mobile Kommunikationsstationen eingesetzt[3].

Zusammenfassend lässt sich sagen, dass das Ziel der im Rahmen des Krisenmanagementsystems durchgeführten Maßnahmen die Aufrechterhaltung der Kontinuität der Führung und die „Gewährleistung einer hohen Verfügbarkeit und Zuverlässigkeit von Informationssystemen, Diensten und Informationen sowie der Integrität, Vertraulichkeit und Authentizität der Informationen, die eine reibungslose Realisierung der Hauptziele der Mission und die Steuerung des Vertrauens in die Missionspartner ermöglichen"[4] ist. Dieses Postulat ist auch für das Untersuchungsgebiet, d.h. das Gebiet der Doppelstadt Frankfurt (Oder) und Słubice, aktuell. Die grenzüberschreitende Problematik der Zusammenarbeit von öffentlicher Verwaltung, Diensten, Inspektionen und Feuerwehren stellt ein interessantes, wenngleich nicht einfaches Forschungsfeld dar. Veränderungen in solchen Gebieten können sehr häufig auftreten, aber auch auf zahlreiche Barrieren stoßen, die sich u. a. aus den unterschiedlichen Organisationskulturen der Verwaltungen, der unterschiedlichen Form des Staates und der öffentlichen Verwaltungssysteme oder aus Sprachbarrieren und anderen ergeben.

Zur Beschreibung eines gut funktionierenden Systems in der wissenschaftlichen und publizistischen Literatur wird der Begriff Widerstandsfähigkeit (Resilienz) verwendet. Sie wird als fehlende Anfälligkeit gegenüber Bedrohungen aus dem äußeren Umfeld des Systems sowie aus seinem Inneren verstanden. Die Einführung dieses Begriffs erweitert die analytischen Möglichkeiten erheblich und erlaubt eine bessere Veranschaulichung möglicher destabilisierender Situationen, von Maßnahmen zur Erhöhung der Widerstandsfähigkeit oder zur Erhöhung der Anfälligkeit gegenüber Bedrohungen. Angesichts des Forschungsgegenstandes konzentrierte sich die Aufmerksamkeit der Forscher auf die Fragen der Cybersicherheit der öffentlichen Verwaltung und der im grenzüberschreitenden Gebiet zusammenarbeitenden Akteure sowie auf mögliche Kommunikationsbarrieren in diesem Bereich und Wege zu deren Überwindung.

1.1. Resilienz der öffentlichen Verwaltung gegenüber Cyberbedrohungen[5]

Die öffentliche Verwaltung bildet das Fundament für das Funktionieren des Staates, und ihre digitale Widerstandsfähigkeit ist zu einer Voraussetzung für soziale und wirtschaftliche Stabilität geworden. Durch die Digitalisierung, die Entwicklung von E-Government-Diensten und den Datenaustausch werden Behörden, zentrale Institutionen und Kommunalverwaltungen immer häufiger zum Ziel von

3 Bericht über die Operation FENIKS, S. 14 (eigene Quelle).

4 M. Popis, A. Bajda, D. Laskowski, Wybrane aspekty bezpieczeństwa informacyjnego w systemie reagowania kryzysowego (Ausgewählte Aspekte der Informationssicherheit im Krisenreaktionssystem), [in:] G. Sobolewski, D. Majchrzak (Hrsh.), Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego (Krisenmanagement im nationalen Sicherheitssystem), Akademia Obrony Narodowej, Warszawa 2011, s. 76.

5 Verfasser: K. Glejt.

Cyberangriffen. Im Gegensatz zum privaten Sektor trifft ein Angriff auf die öffentliche Verwaltung nicht nur die technologische Infrastruktur, sondern vor allem das Vertrauen der Bürger in den Staat. Der Verlust dieses Vertrauens kann sich als kostspieliger erweisen als die Ausgaben für die Wiederherstellung der Systeme.

Die Geschichte der letzten Jahre bestätigt, dass die öffentliche Verwaltung besonders anfällig für Ransomware-Angriffe ist. Ein Fall aus den Vereinigten Staaten, aus Baltimore aus dem Jahr 2019, wo die Malware „RobbinHood“ die Server der Stadt für fast drei Wochen blockierte, verdeutlichte das Ausmaß des Problems – die Gesamtkosten des Vorfalls beliefen sich auf über 18 Millionen Dollar, und die Einwohner spürten die Auswirkungen noch viele Monate lang. In Polen ist die Gemeinde Zambrów ein Beispiel für einen Ransomware-Angriff, bei dem 2022 mangelnde Schulungen, Tests und Backups zu einem schwerwiegenden Ransomware-Vorfall führten, der zusätzlich mit einer Geldstrafe durch die Datenschutzbehörde geahndet wurde. In Oakland stahlen Kriminelle im Jahr 2023 mehr als 600 Gigabyte an Finanz- und Gesundheitsdaten von Verwaltungsmitarbeitern, was zeigt, dass Datendiebstahl und Identitätsdiebstahl genauso gefährlich sind wie die Lähmung von Systemen.

Nicht weniger gefährlich sind DDoS-Angriffe, die digitale Dienste durch Überlastung der Server mit massiven Anfragen lahmlegen. In Deutschland wurde 2023 in Hannover die Website der Polizei von Niedersachsen Opfer eines DDoS-Angriffs, und einige Monate später wurde das S-Bahn-System lahmgelegt. Ähnliche Probleme traten in Polen auf, unter anderem in Olsztyn, wo ein Angriff auf das zentrale Verkehrsleitsystem und mobile Tickets den öffentlichen Nahverkehr lahmlegte. Vorfälle dieser Art zeigen, dass es nicht immer komplizierter Tools bedarf, um die Funktionsfähigkeit der Verwaltung zu beeinträchtigen – eine Überlastung der Infrastruktur reicht aus.

Phishing und Social Engineering sind weitere gängige Angriffsmethoden, die aufgrund des menschlichen Faktors besonders gefährlich sind. Gefälschte E-Mails oder SMS-Nachrichten zielen darauf ab, Daten zu stehlen oder zur Installation von Schadsoftware zu verleiten. Im Jahr 2023 kam es in Posen zu einem Datenleck einer SMS-Datenbank mit den Daten von 30.000 Einwohnern, was zeigt, dass selbst einfache Kommunikationsmechanismen zu schwerwiegenden Verstößen führen können. Ein noch spektakuläreres Beispiel ist der weltweite Angriff WannaCry im Jahr 2017, der die Systeme der Deutschen Bahn in Deutschland lahmlegte und zeigte, wie groß die Gefahr durch ungepatchte Schwachstellen und erst recht durch vom Hersteller nicht mehr unterstützte Betriebssysteme, in diesem Fall Windows XP, ist.

Neben den traditionellen technischen Gefahren gewinnt auch der Bereich des Informationsaustauschs zunehmend an Bedeutung. **Desinformation und Fake News** greifen nicht direkt die Systeme an, sondern untergraben die Glaubwürdigkeit der Verwaltung. Falsche Meldungen, die während Gesundheits- oder Migrationskrisen verbreitet werden, führen zu sozialem Chaos, Vertrauensverlust und Verzögerungen bei Hilfsmaßnahmen. Im Zeitalter der sozialen Medien kann sich Desinformation schneller verbreiten als offizielle Mitteilungen staatlicher Institutionen.

Die im weiteren Verlauf des Berichts vorgestellten Umfrageergebnisse bestätigen, dass die größten Befürchtungen der Befragten Phishing, DDoS-Angriffe und Datenlecks sind. Über 60 % der Befragten geben an, dass sie die Verfahren zur Reaktion auf Vorfälle kennen, aber nur ein Fünftel gibt zu, dass in ihren Institutionen regelmäßig Penetrationstests durchgeführt werden. **Das bedeutet, dass in der Verwaltung das Phänomen des „optimistischen Irrtums” auftritt: Die hohe Selbsteinschätzung**

der Sicherheit findet in der Praxis keine Bestätigung. In derselben Umfrage wurde festgestellt, dass die wichtigsten technologischen Anforderungen die Kommunikation und der Informationsaustausch, Warnungen und Alarme sowie die Darstellung der Situation in Echtzeit sind. Das bedeutet, dass Resilienz nicht nur als eine Frage der technischen Sicherheit angesehen wird, sondern vor allem als die Fähigkeit zur schnellen, mehrkanaligen Kommunikation.

Auch gesetzliche Regelungen beeinflussen die Widerstandsfähigkeit der Verwaltung. Das Gesetz über das nationale Cybersicherheitssystem[6] verpflichtet öffentliche Einrichtungen zum Schutz ihrer IT-Systeme und zur Meldung von Vorfällen. Der nationale Interoperabilitätsrahmen definiert Mindestanforderungen an die Sicherheit von Verwaltungssystemen, darunter den Schutz der Datenintegrität und die Kohärenz der Verfahren. Die NIS2-Richtlinie, die in Form einer Novelle des Gesetzes über das nationale Cybersicherheitssystem in polnisches Recht umgesetzt wird, erweitert den Katalog der Unternehmen, die den Verpflichtungen im Bereich der Cybersicherheit unterliegen, und führt strenge Anforderungen in Bezug auf Risikomanagement, Audits und die Verantwortung der Geschäftsleitung ein. In der Praxis bedeutet dies, dass die **öffentliche Verwaltung nicht reaktiv handeln darf, sondern langfristige Strategien im Einklang mit dem Rechtsrahmen entwickeln muss, wobei Versäumnisse nicht nur zu finanziellen Verlusten, sondern auch zu Verwaltungsstrafen und persönlicher Haftung führen können.**

Das zentrale Problem bleibt jedoch die Finanzierung dieser Maßnahmen. Viele lokale Behörden und kleinere Ämter verfügen nicht über die Mittel für die Modernisierung ihrer Systeme, die Einstellung von Fachpersonal oder regelmäßige Audits oder Penetrationstests. Der Aufbau der Widerstandsfähigkeit solcher Systeme, die die Erfüllung öffentlicher Verwaltungsaufgaben unterstützen, erfordert eine stabile finanzielle Unterstützung durch den Staat und europäische Fonds, damit Cybersicherheit nicht als Kostenfaktor, sondern als strategische Investition in das Vertrauen und die Sicherheit der Bürger betrachtet wird. Beispiele für Programme zur Unterstützung lokaler Behörden bei der Verbesserung ihrer Cybersicherheitsfähigkeiten sind das Projekt „Digitale Gemeinde" und „Cybersichere Selbstverwaltung", die aus europäischen Mitteln finanziert werden.

Die Bewertung der Widerstandsfähigkeit der Verwaltung sollte auf objektiven Indikatoren basieren. Die durchschnittliche Zeit bis zur Erkennung eines Vorfalls (**MTTD** – mean time to detect), die durchschnittliche Reaktionszeit (**MTTR** – mean time to respond), der Prozentsatz der in den letzten zwölf Monaten geprüften Systeme oder der Ausbildungsstand der Mitarbeiter im Bereich Cyberhygiene sind Messgrößen, mit denen die tatsächliche Wirksamkeit der Maßnahmen überwacht werden kann. Nur mit solchen Indikatoren ist es möglich, verschiedene Verwaltungseinheiten zu vergleichen und Investitionen auf der Grundlage von Daten zu planen.

Auch die Zukunftsperspektive ist nicht ohne Bedeutung. Cyberkriminelle nutzen zunehmend künstliche Intelligenz, um Phishing zu automatisieren, glaubwürdige Nachrichten zu generieren oder *Deepfakes* zu erstellen, die sich als Beamte, Stadtverwalter oder Politiker ausgeben. Um sich auf diese Herausforderungen vorzubereiten, sollte die Verwaltung nicht nur eigene KI-Tools entwickeln, wie z. B. lokale Sprachmodelle für Übersetzungen und zweisprachige Kommunikation, sondern auch lernen, von künstlicher Intelligenz generierte Bedrohungen zu erkennen. In Zukunft werden KI-gestützte

[6] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Gesetz vom 5. Juli 2018 über das nationale Cybersicherheitssystem), GBl. 2018 Nr. 1560.

Analysezentren eine Schlüsselrolle bei der Überwachung nicht nur technischer, sondern auch informativer Risiken spielen und der Verwaltung ein vollständigeres Bild der Krisensituation vermitteln.

Zusammenfassend lässt sich sagen, dass die Widerstandsfähigkeit der öffentlichen Verwaltung gegenüber Cyberbedrohungen ein Prozess der kontinuierlichen Anpassung und des Lernens ist. Beispiele aus Baltimore, Oakland, Hannover oder Zambrów zeigen, dass mangelnde Vorbereitung zu Verlusten in Millionenhöhe und zum Verlust des Vertrauens der Öffentlichkeit führt.

Die im weiteren Verlauf dieses Berichts vorgestellten Forschungsergebnisse bestätigen wiederum, dass Personen, die in der öffentlichen Verwaltung tätig sind, sich der Gefahren bewusst sind, dies jedoch selten in systematische Maßnahmen und objektive Tests der Widerstandsfähigkeit umsetzen. In den kommenden Jahren wird es voraussichtlich entscheidend sein, moderne Technologien, gesetzliche Regelungen, bewusstes Management, Mitarbeiterschulungen und stabile Finanzierungsmechanismen miteinander zu verbinden. Nur durch die Synergie dieser Elemente kann die öffentliche Verwaltung ihre Rolle als Garant für Sicherheit und Stabilität in Zeiten digitaler Bedrohungen und Herausforderungen erfüllen, ohne dabei den wirksamen technologischen Wandel zu bremsen, sondern vielmehr zu fördern.

Der Aufbau der Widerstandsfähigkeit der öffentlichen Verwaltung im grenzüberschreitenden Bereich erfordert nicht nur moderne technologische Instrumente und rechtliche Rahmenbedingungen, sondern auch klar definierte Rollen, Zuständigkeiten und Koordinierungsmechanismen. Die Erfahrungen der letzten Jahre zeigen, dass Krisen - sowohl digitaler als auch physischer Natur - über Staatsgrenzen hinausgehen und dass ihre wirksame Bewältigung kohärente Verfahren und neutrale Strukturen zur Unterstützung der Zusammenarbeit erfordert. In diesem Zusammenhang ist es besonders wichtig, bewährte Verfahren aus ausgereiften Branchen wie IT oder Cybersicherheit zu übertragen und Prozessinstrumente anzupassen, die die Transparenz und Vorhersehbarkeit von Maßnahmen erhöhen.

Ein besonders wichtiger Aspekt beim Aufbau von Resilienz im grenzüberschreitenden Bereich ist die Schaffung der Rolle eines Sicherheitsarchitekten, der als unabhängiger und neutraler Experte fungieren würde. Seine Aufgabe wäre es, die Prozesse der grenzüberschreitenden Zusammenarbeit aus einer systemischen Perspektive zu betrachten, die frei von politischen oder organisatorischen Bedingungen ist. Diese Person wäre für die Identifizierung von Bedrohungen im digitalen und physischen Bereich, die Modellierung potenzieller Angriffsvektoren und die Entwicklung von Krisenszenarien verantwortlich – sowohl der wahrscheinlichsten als auch der extremsten, aber realistischen. Der Sicherheitsarchitekt würde auch Reaktions- und Präventionsmechanismen aufzeigen und Empfehlungen zur Erhöhung des Sicherheitsniveaus der öffentlichen Verwaltung und der kooperierenden Institutionen auf beiden Seiten der Grenze formulieren. Die Neutralität und Unpolitizität dieser Rolle würde dem Aufbau von Vertrauen zwischen nationalen und ausländischen Partnern förderlich sein, und die Empfehlungen würden auf der Grundlage einer objektiven Risikoanalyse und nicht aufgrund momentaner politischer Erfordernisse erstellt werden.

Ein guter Bezugspunkt für den Aufbau von Reife im Krisenmanagement kann die IT-Branche und der Cybersicherheitssektor sein, die sich seit Jahren durch ein hohes Maß an Prozessreife auszeichnen. Dies liegt daran, dass diese Organisationen bereits früher mit Bedrohungen konfrontiert waren, oft unabhängig von staatlichen Vorschriften handelten und ihre Aktivitäten durch geschäftliche Vorteile motiviert waren – den Schutz ihres Rufs und die Minimierung finanzieller Verluste. Infolgedessen hat der Cybersicherheitssektor einen kohärenten Rahmen für die Reaktion auf Vorfälle entwickelt, der heute

der Verwaltung als Vorbild dienen kann. Eine wichtige Rolle spielen auch EU-Institutionen wie ENISA oder das EU-Netzwerk CyCLONe, die für die transnationale Koordinierung zuständig sind, sowie Referenzinstrumente wie die MITRE ATT&CK-Matrix, die das Wissen über die Taktiken und Techniken von Cyberkriminellen systematisiert und auch auf einen breiteren Krisenkontext angepasst werden kann. Über alle Vorfälle wachen sektorale CSIRT-Teams, die Ereignisse überwachen, analysieren und bearbeiten und gleichzeitig Verfahren entwickeln, die die Widerstandsfähigkeit der Organisation auf lange Sicht erhöhen.

Eine wichtige Ergänzung zu den oben genannten Mechanismen ist der Einsatz von Prozesswerkzeugen wie der RACI-Matrix. Diese einfache und zugleich effektive Lösung ermöglicht es, klar zu definieren, wer für die Ausführung von Aufgaben verantwortlich ist (Responsible), wer für die endgültigen Entscheidungen zuständig ist (Accountable), wer als Berater fungiert (Consulted) und wer informiert werden sollte (Informed). In einer Krisensituation an der polnisch-deutschen Grenze ermöglicht die Anwendung der RACI-Matrix eine schnelle und eindeutige Aufteilung der Aufgaben zwischen den Partnern, wodurch Chaos aufgrund mangelnder Entscheidungsfähigkeit oder Doppelarbeit vermieden wird. Dadurch wird der Reaktionsprozess transparenter, übersichtlicher und auch bei Übungen oder Tests reproduzierbar. Langfristig fördert die RACI-Matrix den Aufbau von Vertrauen zwischen den Institutionen, da sie das Risiko einer Unklarheit der Verantwortlichkeiten beseitigt.

Tabelle 1. Beispielhafte Anwendung der RACI-Matrix für den Bereich der Doppelstadt Słubice und Frankfurt (Oder)

Aufgabe	**Feuer-wehr (PL)**	**Feuer-wehr (DE)**	**Stadt-verwal-tung (PL)**	**Stadt-verwal-tung (DE)**	**Krisen-stab (PL)**	**Krisen-stab (DE)**	**Medien / Public Relations**
Identifizierung der Gefahr	R	R	I	I	A	A	I
Benachrichtigung der Dienste	C	C	A	A	R	R	I
Koordination grenzüberschreitender Maßnahmen	C	C	C	C	A	A	I
Evakuierung der Bevölkerung	R	R	A	A	C	C	I
Kommunikation mit den Medien	I	I	C	C	R	R	R
Abschlussbericht und Analyse	C	C	A	A	A	A	I

Quelle: Eigene Ausarbeitung.

Die Integration der Rolle des Sicherheitsarchitekten, bewährter Verfahren aus der Cybersicherheitsbranche, internationaler Strukturen wie ENISA oder EU CyCLONe und Prozesswerkzeuge wie MITRE ATT&CK oder RACI schafft ein kohärentes Krisenmanagement-Ökosystem. Die grenzüberschreitende Zusammenarbeit im Bereich der Sicherheit erfordert nämlich nicht nur Technologien und rechtliche Rahmenbedingungen, sondern vor allem klare Verantwortungsstrukturen und neutrale Koordinierungsmechanismen. Nur dann wird die öffentliche Verwaltung auf beiden Seiten der Grenze in der Lage sein, wirksam auf Bedrohungen zu reagieren, systemische Widerstandsfähigkeit aufzubauen und das Vertrauen der Bürger angesichts wachsender Herausforderungen aufrechtzuerhalten.

1.2. Resilienz von Krisenmanagementsystemen

Die Widerstandsfähigkeit von Krisenmanagementsystemen kann in vielen Zusammenhängen verstanden werden. Erstens als Verfügbarkeit der notwendigen und ausreichenden Ressourcen für reaktive Maßnahmen in einer Krisensituation. Zweitens als eine Reihe von Sicherheitsmaßnahmen, die darauf abzielen, das Auftreten einer Krisensituation zu verhindern oder Verluste zu reduzieren, wenn das Risiko eintritt. Drittens im Zusammenhang mit der effizienten Wiederherstellung der Funktionsfähigkeit eines durch eine Krise gestörten Systems. Mit der Verbreitung neuer Technologien, der Digitalisierung der öffentlichen Verwaltung und nun auch der Verbreitung von Instrumenten der sogenannten künstlichen Intelligenz eröffnet uns die Reihe von Risiken, die mit ihrer Funktionalität und ihrem störungsfreien Betrieb verbunden sind, nicht nur ein neues Forschungsfeld, sondern auch einen Bereich praktischer Maßnahmen, die durch den Austausch von Erfahrungen und gegenseitige Unterstützung gefördert werden. Ein solcher Ansatz für die Risiken der grenzüberschreitenden Zusammenarbeit unter Einsatz von KI-Tools ist jedoch nach Einschätzung des Teams nicht ausreichend.

Daher wurde auch ein psychologisches und soziologisches Verständnis von Risiko angenommen, bei dem der Faktor Angst als emotionaler Faktor[7] die Risikowahrnehmung beeinträchtigen und in der Praxis auf das in der Verwaltung bekannte Phänomen des „Optimismusfehlers" zurückgeführt werden kann. Denn „die menschliche Erkenntnis und Wahrnehmung [von Risiken – Anm. M. T.] wird nicht nur von dem beeinflusst, was man weiß und versteht, also allgemein gesagt von der Realität, sondern auch von der Kultur und den Bedeutungen"[8], die wir bestimmten Normen, Werten und Einstellungen von Mitarbeitern zuschreiben.

Das Forschungsteam ging von einem vielschichtigen Verständnis des Risikos aus. Zunächst ging es davon aus, dass das Risiko anhand der Wahrscheinlichkeit seines Eintretens und des Ausmaßes der Auswirkungen dieses Ereignisses gemessen wird.[9] Diese Denkweise setzt voraus, dass es Gefahren gibt, die unter bestimmten Umständen, Ereignissen und Fakten eintreten und zu einer Krisensituation führen.

Es ist jedoch nicht zu übersehen, dass die Gesamtheit der Fachbereiche des Risikomanagements angesichts des bedeutenden technologischen und informativen Fortschritts um die Bereiche IT-Risikomanagement und Risikomanagement im Zusammenhang mit der Informationssicherheit ergänzt werden muss.[10] Innerhalb dieses Bereichs sollten die Schlüsselbereiche des Risikomanagementprozesses unter anderem auf folgende Punkte reduziert werden:

- Bereitstellung einer IT-Infrastruktur, die IT-Sicherheit und Datenschutz gewährleistet,
- Erstellung eines Plans zur Aufrechterhaltung des Betriebs im Falle von Störungen,
- Lösungen für die Erbringung von Dienstleistungen mit einer zuverlässigen Kommunikationsinfrastruktur[11].

7 Vgl. J. Arnoldi, Ryzyko, Wydawnictwo Sic!, Warszawa 2011, S. 27.

8 Ibidem, S. 27.

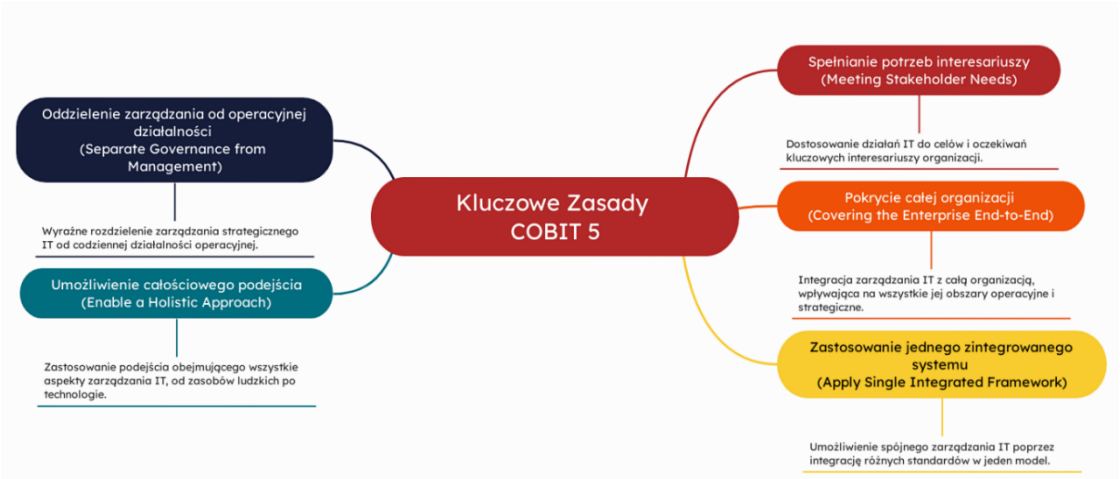
9 Vgl. Ibidem, S. 26.

10 Vgl. C. Thomosn, P. Hopkin, Podstawy zarządzania ryzykiem. Jak wdrażać efektywne systemy zarządzania ryzykiem w przedsiębiorstwie (Grundlagen des Risikomanagements. Wie man effektive Risikomanagementsysteme in einem Unternehmen implementiert), Wydawnictwo Helios, Warszawa 2024, S. 70.

11 Vgl. Ibidem, S. 71.

Ein Überblick über bekannte Methoden und Risikomanagementsysteme in verschiedenen Organisationen zeigt, dass das COBIT-Risikomanagementsystem im Bereich der IT-Sicherheit weit verbreitet ist.[12] Ein charakteristisches Merkmal dieser Norm ist ihr Ansatz, der die Integration verschiedener Systeme in ein einziges, gemeinsam verwaltetes und gemeinsam identifizierbares System in Bezug auf Risiken im Zusammenhang mit den Werten der Organisation, den Personalressourcen, der IT-Infrastruktur und der Kommunikationssicherheit ermöglicht.

Abbildung 1. Die wichtigsten Grundsätze von COBIT 5



Quelle: M. Malinowski, COBIT. IT-Management für Organisationen, https://www.drmalinowski.edu.pl/posts/3249-cobit-zarzadzanie-it-dla-organizacji (Zugriff: 10.08.2025).

Mit dem technologischen und informatischen Fortschritt sowie der zunehmenden Verbreitung des Internets entstanden IT-Tools zur Unterstützung der Führung von Dienst-, Inspektions- und Wachdienststellen. Sie werden als Führungsunterstützungssysteme bezeichnet. Die Kommunikation zwischen verschiedenen Einheiten, die meist über unterschiedliche Unterstützungssysteme verfügen, sollte durch integrierte Kommunikationssysteme der Führungsunterstützungssysteme gewährleistet werden. Es ist zu erwarten, dass mit dem Aufbau eines nationalen Krisenmanagementsystems auf der Grundlage einer Zusammenführung von Diensten, Inspektionen und Wachdiensten die lokalen Verwaltungsbehörden über solche Telekommunikations- und IT-Lösungen verfügen werden, die ihnen die Kommunikation mit den Diensten und den Diensten untereinander ermöglichen. Leider streben wir aus vielen Gründen weiterhin solche Standards an.

Darauf weisen die Autoren des Berichts hin, der die operativen Maßnahmen der Aktion FENIKS zusammenfasst. Sie schreiben über das unzureichende Bewusstsein für Krisenmanagement unter den Beamten der lokalen Verwaltungsbehörden, was sich auf die geringe Wirksamkeit der Maßnahmen in den von der Krise betroffenen Gebieten auswirkt. Sie weisen auch auf den Mangel an laufender Information zwischen den Institutionen über die Krisensituation und die unzureichende Kommunikation mit der lokalen Bevölkerung hin. Eine weitere Erkenntnis aus den operativen Maßnahmen von FENIKS ist das Bewusstsein für den Mangel an Integrationsinstrumenten, die das Krisenmanagement, die Kommunikation und die Verbindung zwischen den Streitkräften und dem nichtmilitärischen System

[12] Über das COBIT-System schreibt unter anderem M. Malinowski, COBIT. Zarządzanie IT dla organizacji, https://www.drmalinowski.edu.pl/posts/3249-cobit-zarzadzanie-it-dla-organizacji (Zugang: 10.08.2025).

zusammenhalten, was zu einer inkonsistenten Darstellung der Krisensituation für die Teilnehmer führte, die Aufgaben im Rahmen der Krisenbewältigungsmaßnahmen durchführten.[13] Im Zusammenhang mit dem Thema dieser Studie ist noch ein weiterer Aspekt hervorzuheben, nämlich der Einfluss neuer Technologien. Darauf weist unter anderem Jakob Arbold hin, wenn er schreibt: „Die zunehmende Nutzung von Technologien zwingt uns dazu, grundlegende Werte und Ansichten darüber kritisch zu überdenken, wo die Unvorhersehbarkeit der Natur endet und wo die Verantwortung des Menschen beginnt"[14] und der Institution, bei der er beschäftigt ist.

Eine der Schlussfolgerungen aus den Untersuchungen, die Gegenstand dieser Studie sind, ist die Notwendigkeit, ein Krisenmanagementsystem zu entwickeln und zu implementieren, das alle Elemente des Systems integriert und IT-Tools nutzt. Die Verwendung von KI-Tools für diesen Zweck sollte mit Vorsicht betrachtet werden. Diese Skepsis ist durch die Haltung der Begünstigten gegenüber solchen Tools bedingt. Sie darf jedoch die potenzielle Möglichkeit des Einsatzes von KI in diesem Bereich nicht ausschließen.

Aus Sicht der Entscheidungsträger, die sich auf Unterstützungssysteme für die Führung stützen, ist deren Zuverlässigkeit von entscheidender Bedeutung, damit die Kontinuität der Führung sowohl bei nicht außergewöhnlichen Präventions- und Überwachungsmaßnahmen als auch in Ausnahmesituationen gewährleistet ist. Derzeit gibt es auf dem polnischen Markt viele Systeme dieser Art. Sie unterscheiden sich in mehreren Punkten, wie z. B. dem Betriebssystem, auf dem sie laufen, der Menge der Daten, die gesammelt und analysiert werden können, der Qualität der grafischen Darstellung des Einsatzgebiets und der Lesbarkeit auf verschiedenen Geräten. Die Standardfunktionen dieser Systeme lassen sich wie folgt zusammenfassen:

- Möglichkeit der Koordinierung und Unterstützung von Maßnahmen,
- Erkennung und Darstellung auf digitalen Kartenunterlagen,
- Erstellung und Übermittlung von Textnachrichten,
- Funktionieren im Offline-Modus,
- Simulation von Maßnahmen,
- Darstellung der Einsatz-/Notfallsituation,
- Planung, Unterstützung und Koordinierung von Maßnahmen,
- sicherer Informationsaustausch (auch vertrauliche Informationen),
- automatische und laufende Berichterstattung,

[13] Vgl. Bericht über die Operation FENIKS, S. 16 und 17 (eigene Quelle).
[14] J. Arnold, *Ryzyko*, *op. cit.*, S. 23.

- Gruppenbenachrichtigung und Alarmierung,
- Sammlung, Verarbeitung und Weitergabe von Informationen über durchgeführte Rettungsmaßnahmen und andere mehr.

Die Sicherheitsarchitektur eines solchen Systems sollte auf folgenden Säulen basieren:

- Zugänglichkeit von Informationen, Ressourcen und Nutzung der Systemdienste,
- Sicherheit des Informationsflusses, der einen schnellen Informationsaustausch zwischen den Einheiten unterstützt,
- kontrollierter Zugang zum Schutz vor unbefugtem Zugriff,
- Datenintegrität mit der Möglichkeit, Sicherheitsvorfälle sofort zu melden,
- ein System zur Authentifizierung und Vertraulichkeit von Daten, das die Identifizierung von Personen ermöglicht, die den Zugriff auf bestimmte Datensätze haben,
- Vertrauen, das die Privatsphäre von Daten unterstützt, verstanden als Überwachung und Exklusivität bei der Verfügung über Daten, die Unternehmen teilen wollen oder müssen[15].

Angesichts des Gebietes, in dem das Projekt durchgeführt wird, können die oben genannten Funktionen unzureichend sein. Jedes Telekommunikations- und Informationssystem muss nämlich die Kompetenzen, aber auch den Tätigkeitsbereich der Einheit berücksichtigen, deren Arbeit unterstützt werden soll. Die Funktionalität eines solchen Systems muss auf Regeln basieren, die das Ausmaß der damit verbundenen Risiken berücksichtigen. Diese Regeln sollten in die Umgebung der Institution implementiert werden und mit denen übereinstimmen, die in anderen, miteinander kooperierenden Einheiten gelten. Aufgrund des grenzüberschreitenden Charakters des Gebiets, in dem eine Notsituation auftreten kann, gelten diese Regeln in Institutionen, die in unterschiedlichen Rechtsordnungen und mit unterschiedlichen internen Organisationskulturen arbeiten. Dies ist eine der größten organisatorischen und administrativen Herausforderungen. Die Nichtbeachtung dieser offensichtlichen Tatsache ist eine der wesentlichen Gefahren für die Funktionsstörung eines solchen Systems.

Die grenzüberschreitende Region Słubice und Frankfurt (Oder) ist durch das Auftreten von außergewöhnlichen Ereignissen gekennzeichnet, deren Art und Ausmaß die Planung und Koordinierung der Maßnahmen von Behörden und öffentlichen Verwaltungen zweier unterschiedlicher Verwaltungsordnungen, Zuständigkeiten und operativer Unterstellungen erfordern kann. Dies können folgende Situationen sein:

15 M. Popis, A. Bajda, D. Laskowski, Wybrane aspekty bezpieczeństwa informacyjnego... (Ausgewählte Aspekte der Informationssicherheit...), op. cit., S. 83.

- Luft- und Wasserverschmutzung (z. B. Smog, Austritt von Chemikalien in Flüsse, die durch mehrere Länder fließen),
- Naturkatastrophen mit grenzüberschreitenden Auswirkungen (z. B. Waldbrände, Überschwemmungen),
- Auswirkungen des Klimawandels (z. B. Klimamigration, Dürren),
- Ausbreitung von Infektionskrankheiten (z. B. COVID-19, Vogelgrippe, SARS, Tuberkulose, ASF),
- mangelnde Koordinierung der Präventions- und Gesundheitsmaßnahmen zwischen den Staaten,
- Brände im Grenzgebiet,
- Massenmigration aufgrund von Krieg, Armut und Klimawandel,
- Hackerangriffe auf kritische Infrastrukturen,
- Verbreitung von Desinformation und Propaganda über soziale Medien,
- internationaler Handel mit Menschen, Drogen und Waffen,
- Aktivitäten grenzüberschreitender krimineller Gruppen.

Die Zusammenarbeit von Behörden und öffentlicher Verwaltung im grenzüberschreitenden Raum ist mit zahlreichen Herausforderungen verbunden, die zu Hindernissen für die Zusammenarbeit werden können. Bei einer kurzen Charakterisierung der bisherigen Bereiche der Zusammenarbeit an der polnisch-deutschen Grenze wird auf die in diesem Zusammenhang bedeutenden kulturellen Barrieren, negativen Stereotypen, historischen Erfahrungen und die Unkenntnis der Sprache des Nachbarn hingewiesen. Die grenzüberschreitende Zusammenarbeit ist zwar durch die Entwicklung der Zusammenarbeit zwischen Gebietskörperschaften, Schulen und Kulturinstitutionen sowie der Wirtschaftsverwaltung gekennzeichnet, jedoch bei gleichzeitig geringem Sozialkapital. Die Oder, die eine natürliche Grenze zwischen den beiden Staaten bildet, „könnte zu einem wichtigen Impulsgeber für die Zusammenarbeit z. B. in den Bereichen Umweltschutz, Katastrophenschutz, Wirtschaftsprojekte und Tourismus werden"[16]. Zu diesen Bereichen der Zusammenarbeit kommt noch die Zusammenarbeit im Bereich des Krisenmanagements hinzu. Diese Perspektive erfordert eine Betrachtung der Region als funktionale Einheit, als eine Ansammlung von Menschen, die in einem bestimmten Gebiet leben, für

[16] S. Dołzbłasz, A. Raczyk, Projekty współpracy transgranicznej na zewnętrznych i wewnętrznych granicach Unii Europejskiej – przykład Polski (Projekte der grenzüberschreitenden Zusammenarbeit an den Außen- und Binnengrenzen der Europäischen Union – das Beispiel Polen), „Studia Regionalne i Lokalne" nr 3(45), 2011, S. 64.

dessen Sicherheit öffentliche Verwaltungsstellen eingerichtet wurden, von deren Zusammenarbeit die Sicherheit dieses Gebiets abhängt.

Das Vorhandensein von Hindernissen in der Zusammenarbeit zwischen Behörden, Inspektionen und Wachdiensten sowie Kommunal- und Landesverwaltungen wirkt sich negativ auf die Sicherheit der in diesem Gebiet lebenden Bevölkerung aus. Darüber hinaus handelt es sich um Faktoren und Situationen, deren Auftreten die Widerstandsfähigkeit des Krisenmanagementsystems beeinträchtigt. Eine Gesamtanalyse zeigt, dass diese sehr unterschiedlicher Natur sein können. Paradoxerweise werden mit dem technologischen Fortschritt einige Hindernisse, unter anderem in Bezug auf die Übertragung, Sammlung von Informationen, Fernkommunikation, Echtzeit-Videoüberwachung und andere, beseitigt. Es entstehen jedoch neue Hindernisse, die ebenfalls beseitigt werden können, z. B. mit Hilfe von KI-Tools. Für die Zwecke des Projekts wurden mögliche Hindernisse für die grenzüberschreitende Zusammenarbeit identifiziert:

- eine Struktur der Zuständigkeitsverteilung zwischen Behörden und Verwaltungen, die nicht an die grenzüberschreitenden Gegebenheiten angepasst ist,
- Unmöglichkeit der Datenübermittlung im grenzüberschreitenden Bereich aufgrund der DSGVO,
- Fehlen gemeinsamer Pläne und Verfahren für Krisensituationen bei grenzüberschreitenden Notfällen,
- Fehlen politischer Unterstützung für die grenzüberschreitende Zusammenarbeit der Behörden,
- Nichtdurchführung von Präventivmaßnahmen in identifizierten Notfällen,
- Fehlendes Engagement ausländischer Partner bei der Krisenplanung,
- Rechtliche Beschränkungen beim Grenzübertritt von Mitarbeitern von Behörden, Inspektionen und Wachdiensten (z. B. grenzüberschreitende Verfolgungen),
- Fehlen einheitlicher Vorschriften für die Anwendung von Gewalt, Festnahmen oder Durchsuchungen,
- Risiko der Offenlegung geschützter Informationen oder von Missbrauch,
- Rivalität zwischen den Behörden (auch innerhalb eines Landes),
- Schwierigkeiten bei der operativen Kommunikation (Fehlen einer gemeinsamen Arbeitssprache),
- unterschiedliche Organisationskulturen, Führungsstile, Ausrüstung, Schulungen,
- mangelnde Interoperabilität der IT-Systeme (fehlende gemeinsame Datenbanken),

- Probleme beim Datenaustausch in Echtzeit,
- Schwierigkeiten bei der Organisation gemeinsamer Übungen, Schulungen und Operationen,
- ungleicher Zugang zu modernen Kommunikations- und Logistikmitteln,
- unterschiedliche nationale und politische Interessen,
- mangelnde Kenntnisse über die Ausrüstung der operativen Einheiten des Nachbarlandes,
- zeitaufwändige Verfahren, die eine Zusammenarbeit in Echtzeit ermöglichen (Einholung von Genehmigungen oder Weitergabe von Informationen).

Für wissenschaftliche und didaktische Zwecke wurde im Rahmen der im Projekt durchgeführten Aufgaben angenommen, dass eine Krisensituation eine Reihe von Umständen ist, in denen sich ein Unternehmen, ein Teil davon oder ein bestimmter Bereich seiner Tätigkeit befindet. Diese Faktoren können interner und externer, objektiver und subjektiver Natur sein. Ihre Aktivierung kann sich positiv oder negativ auf das Unternehmen auswirken, in jedem Fall jedoch das systemische Gleichgewicht, in dem das Unternehmen funktioniert, stören. Vereinfacht gesagt kann man sagen, dass ein Unternehmen bei Eintritt einer Gefahr vorübergehend oder dauerhaft seine Steuerungsfähigkeit verliert und die Kontrolle über seine Funktionsweise verliert.

Eine Krisensituation kann das Ergebnis beabsichtigter oder unbeabsichtigter Handlungen von Elementen sein, die zusammen das Umfeld des Systems bilden, in dem die Organisation funktioniert. In jedem Fall erfordert diese Situation eine Reaktion, deren Ziel es ist, das Gleichgewicht des jeweiligen Systems, der Organisation, wiederherzustellen. Der Krisenmoment kann für sie sowohl in Bezug auf die damit verbundenen Gewinne als auch Verluste ein Wendepunkt, eine Revolution sein.

Eine derart weit gefasste Definition einer Krisensituation, die auf einem interdisziplinären Ansatz zum Begriff „Krise" basiert, ermöglicht es, zahlreiche Ereignisse zu erfassen, die an den Staatsgrenzen in Regionen auftreten können, die von einem Großteil der Bevölkerung auf beiden Seiten der Grenze bewohnt werden. Die größte Herausforderung für die Erleichterung der Zusammenarbeit zwischen den Einheiten ist weniger die Kohärenz oder Kommunikationsfähigkeit ihrer Führungsunterstützungssysteme als vielmehr die laufende Kommunikation über verschiedene Kanäle zu verschiedenen Ereignissen. Um Situationen zu identifizieren, in denen eine Zusammenarbeit der Dienste beider Länder erforderlich ist, wurden mögliche Umstände festgelegt und im Rahmen von Interviews mit den Studienteilnehmern überprüft.

Das Hauptziel der im Rahmen des Krisenmanagements ergriffenen Maßnahmen ist die Minimierung materieller und menschlicher Verluste sowie die Wiederherstellung der Situation vor der Krise. Diese Maßnahmen werden durch Dienste unterstützt, die über die erforderlichen materiellen und immateriellen Ressourcen verfügen. Neben den bereits genannten Aufgaben besteht ihre Rolle darin, Anweisungen an die Zivilbevölkerung weiterzugeben. Derzeit kann eine Information vom Absender bis zum Empfänger über viele Kanäle gelangen. Aus Sicht der Krisenmanagementtheorie und der Massenkommunikation muss diese Information einheitlich im Inhalt, verständlich, glaubwürdig, leicht verständlich und mit konkreten Verhaltensweisen für die Zivilbevölkerung versehen sein.

Aus Sicht der Projektziele stellt **das Fehlen einer effizienten, verständlichen Kommunikation zwischen den Mitarbeitern der Dienste auf beiden Seiten der Grenze, in diesem Fall der polnisch-deutschen Grenze, einen wesentlichen Risikofaktor dar, der die Möglichkeit einer den Umständen angemessenen Reaktion auf eine Krisensituation dauerhaft beeinträchtigen kann. Aus dieser Perspektive können die Möglichkeiten, die KI im Krisenmanagement bietet, einen positiven Einfluss auf die Zusammenarbeit und Kommunikation der Dienste haben. Eine unsachgemäße Nutzung kann hingegen zu einer weiteren Krisensituation führen, die die negativen Auswirkungen der ursprünglichen Krise noch verschärft. In beiden Fällen sind der Mensch, sein Vertrauen und seine Bereitschaft, seine Arbeit mit KI-Tools zu unterstützen, ein Risikofaktor.**

Die Einführung von KI-Tools für das Krisenmanagement als Unterstützung bei aktuellen und strategischen Entscheidungen ist nur scheinbar eine vorteilhafte Lösung. Damit sind auch Risiken verbunden. In Studien zur Einführung von KI-Tools in den Entscheidungsprozess wird darauf hingewiesen, dass es notwendig ist, Regeln für die Nutzung von KI in Unternehmen oder Behörden zu entwickeln und umzusetzen sowie die Fähigkeiten für den sachgerechten Einsatz dieser Tools zu vermitteln. Die Einführung einer behördlichen Richtlinie für die Nutzung von KI-Tools durch Mitarbeiter kann vor Datenlecks, der Verarbeitung falscher Daten oder Reputationsverlusten schützen. Diese letzte Forderung hängt mit einer für Fachleute offensichtlichen Tatsache zusammen, nämlich dass KI-Tools zwar unterstützen, aber nicht die Arbeit in Schlüsselpositionen des Notfallmanagements ersetzen können. Von Mitarbeitern, die sich mit Krisenmanagement und Katastrophenschutz befassen, sollte daher erwartet werden, dass sie fachlich in der Lage sind, die von KI gelieferten Inhalte zu überprüfen, und erst dann strategische Entscheidungen treffen. Die Kenntnis von KI-Tools wird zu einem Vorteil bei der Arbeit in der Sicherheitsbranche, insbesondere bei der Datenanalyse oder der Automatisierung von Routinetätigkeiten.

Es kann darauf hingewiesen werden, dass die Regeln für die Nutzung von KI-Tools zur Unterstützung des Entscheidungsprozesses unter anderem Folgendes umfassen sollten:

- Identifizierung verbotener Systeme,
- Identifizierung von Systemen mit hohem Risiko,
- Identifizierung von Systemen mit begrenztem Risiko und
- Identifizierung von Systemen mit minimalem Risiko.

Für jedes der oben genannten Systeme sollte der Datenverantwortliche das Verfahren für deren Implementierung, Verwendung, Dokumentation ihrer Verwendung und Dokumentation von KI-gestützten Ereignissen entwickeln. Es ist anzumerken, dass die Rechtsgrundlagen für KI in den Ländern der Europäischen Union grundsätzlich einheitlich sind. Die Unterschiede zwischen Polen und Deutschland beziehen sich auf nationale Rechtsvorschriften zu nationalen Cybersicherheitssystemen und Durchführungsbestimmungen, unter anderem zur Richtlinie 2022/255 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 (NIS 2).

Konrad GLEJT

KAPITEL II. KÜNSTLICHE INTELLIGENZ ALS UNTERSTÜTZUNG FÜR KRISENKOMMUNIKATIONSSYSTEME

2.1. Einführung und Hintergrund

Es ist schwer vorstellbar, dass Grenzgebiete voneinander getrennt sind. Es erscheint nur natürlich, dass sie in einem Umfeld funktionieren, in dem sich die Umstände, einschließlich der Gefahren, dynamisch verändern und oft grenzüberschreitenden Charakter haben. Überschwemmungen, Umweltverschmutzung, Brände, massive Infrastrukturausfälle oder Desinformationskampagnen – all diese Phänomene erfordern eine schnelle Reaktion, die Koordination vieler Akteure und eine effektive Kommunikation mit den Bürgern. Es stellt sich die Frage, wie die heute verfügbaren Instrumente die Arbeit von Behörden, Inspektionen und Wachdiensten unterstützen können, deren Tätigkeiten sich de facto im Alltag überschneiden. Darüber hinaus gehen sie über die Grenzen ihres eigenen Landes hinaus und greifen häufig in die Umgebung ein. Wie können in diesem Zusammenhang künstliche Intelligenz (KI), maschinelles Lernen (ML) und neuronale Netze (ANN) helfen? Und wenn ja, inwiefern?

Die Ergebnisse der im Rahmen des Cross-AI Connect-Projekts im Jahr 2025 durchgeführten Umfrage zeigen, dass:

- 83,2 % der Befragten KI-Tools für ihre tägliche Arbeit als nützlich erachten,
- 68 % sehen das größte Potenzial von KI in den Bereichen Kommunikation, Informationsaustausch sowie Warnung und Alarmierung,
- 44 % sehen das Fehlen einer gemeinsamen Arbeitssprache als wesentliches Hindernis für die Zusammenarbeit,
- 39 % weisen auf die mangelnde Interoperabilität der IT-Systeme hin.

Diese Daten lassen den Schluss zu, dass Technologien der künstlichen Intelligenz eine entscheidende Rolle bei der Beseitigung von Sprachbarrieren und der Verbesserung der Qualität und Geschwindigkeit der Informationsübermittlung in Krisensituationen spielen können. Dies umso mehr, als in solchen Fällen die Reaktionszeit zur wertvollsten Währung wird. Im nächsten Teil werden Übersetzungstools, ihre Möglichkeiten und ihr Potenzial zur Unterstützung des Alltagslebens von grenzüberschreitend aktiven Personen vorgestellt.

2.2. Wie unterstützt KI das Krisenmanagement?

Künstliche Intelligenz im Kontext des Krisenmanagements umfasst nicht nur „intelligente Programme", sondern eine ganze Reihe von Tools und Mechanismen, mit denen sich riesige Datenmengen verarbeiten, wichtige Ereignisse erkennen, Entscheidungen unterstützen und Kommunikation in vielen

Sprachen durchführen lassen. Besonders wichtig ist hier die Vorhersage auf der Grundlage zuvor entwickelter Modelle. Die Analyse zukünftiger Situationen anhand von Daten ist unter Krisenmanagern allgemein bekannt. Es wurden Modelle geografischer Informationssysteme (GIS) verwendet, die auf implantierten Karten, Simulationen und historischen Daten basierten, jedoch standardmäßig nicht durch zusätzliche große Sprachmodelle (LLM) unterstützt werden. In Krisensituationen muss jedoch der Kontext umfassender analysiert werden, insbesondere Daten, Informationen und Erfahrungen, die sich dann auf die Entscheidungsfindung im realen Leben auswirken.

Beispiele für den Einsatz künstlicher Intelligenz:

- **Echtzeitübersetzungen** – Anwendungen und Sprachmodelle für die Übersetzung von Gesprächen, Sprachmitteilungen und Dokumenten im Online- und Offline-Modus. Nicht nur von Texten, sondern auch von Sprachaufnahmen mit entsprechenden Eigenschaften.

- Informationsüberprüfung – KI-Tools analysieren Inhalte in sozialen Medien, erkennen Falschinformationen, Deepfakes (computergenerierte gefälschte Audio- und Videomaterialien) und fehlerhafte Dateninterpretationen. Dabei handelt es sich um sogenannte Honeypot-Tools, also Köder, die Bots automatisch erkennen.

- Entscheidungsassistenten – KI-Systeme können Zusammenfassungen von Berichten erstellen, Vorfälle analysieren, Ereignisse korrelieren und anschließend Handlungsempfehlungen ausarbeiten, z. B. Evakuierungspläne auf der Grundlage von Eingabedaten aus verschiedenen Quellen erstellen. Darüber hinaus können sie quasi autonom Entscheidungen mit geringem Risiko treffen.

2.3. KI in der mehrsprachigen Kommunikation

Die Kommunikation zwischen polnischen und deutschen Behörden ist eine der größten Herausforderungen im Bereich des grenzüberschreitenden Krisenmanagements. Dabei geht es nicht nur um große Naturkatastrophen oder Vorfälle von großem Ausmaß – eine Herausforderung ist auch die tägliche operative Zusammenarbeit, bei der Sprachunterschiede zu Verzögerungen und sogar zu Fehlentscheidungen führen können. Wie die Umfrageergebnisse zeigen, nutzen 16,7 % der Befragten KI-Tools regelmäßig und 61,1 % gelegentlich, was darauf hindeutet, dass diese Technologie allmählich zum Standard wird, der die tägliche Arbeit auch im Bereich der Kommunikation unterstützt.

Der kritischste Aspekt ist das präzise Verständnis der Terminologie, insbesondere in Situationen, in denen es um die Gesundheit und das Leben von Menschen geht. Semantische Missverständnisse (z. B. in der Notfallmedizin, Logistik oder Koordination von Einsatzkräften) können schwerwiegende Folgen haben. Daher spielen KI-Tools für Übersetzungen und Sprachsynthese eine wichtige Rolle, da sie die Effizienz und Geschwindigkeit der Arbeit erheblich steigern können.

Tools zur Unterstützung der Kommunikation:

1. **Ollama mit dem Modell granite3-dense**

   Ollama ist eine Plattform, die es ermöglicht, große Sprachmodelle lokal auszuführen. Das Modell granite3-dense bietet eine hohe Leistung bei der Analyse und Verarbeitung von Text in

Echtzeit. Im Kontext des Krisenmanagements ist es von entscheidender Bedeutung, dass das Modell in einer von öffentlichen Netzwerken getrennten Umgebung betrieben werden kann, was die Sicherheit sensibler Informationen erhöht. Zu den Anwendungsbereichen gehören die automatische Erstellung von Zusammenfassungen von Berichten, Übersetzungen und die Konvertierung von Nachrichten zwischen verschiedenen Sprachen.

2. **PLLuM (Polnisches Großsprachmodell) und Bielik**

Es handelt sich um Sprachmodelle, die auf der Grundlage von Daten in polnischer Sprache trainiert wurden und die Möglichkeit bieten, sie in einer lokalen Infrastruktur zu hosten. PLLuM eliminiert das Risiko von Datenlecks außerhalb der von öffentlichen Institutionen kontrollierten Systeme, was im Kontext der nationalen Sicherheit besonders wichtig ist. Zu seinen Anwendungsbereichen gehören unter anderem die Erstellung spezieller Krisenglossare, die Unterstützung der automatischen Übersetzung von Berichten der Rettungsdienste und die Standardisierung der operativen Terminologie. Bielik basiert auf dem Modell Mistral-7B und ist ein Tool der Stiftung SpeakLeash, die ML und LLM fördert.

3. **Teuken – OpenGPT-X: Teuken 7B – Fraunhofer IAIS**

Unternehmen aus verschiedenen Branchen erhalten neue Möglichkeiten zur Implementierung von Anwendungen auf Basis künstlicher Intelligenz. Auf der Plattform Hugging Face wurde das Modell „Teuken 7B-instruct-v0.4" kostenlos zur Verfügung gestellt, das im Rahmen des Forschungsprojekts OpenGPT-X entwickelt wurde. Es handelt sich um ein umfangreiches Sprachmodell, das von Grund auf in 24 Amtssprachen der Europäischen Union trainiert wurde und dessen Architektur sieben Milliarden Parameter umfasst.

Die neue Lösung kann sowohl von Unternehmen als auch von wissenschaftlichen Einrichtungen genutzt werden. Das Modell kann heruntergeladen und dann an die eigenen Bedürfnisse angepasst werden – indem es mit Fachdaten ergänzt und für bestimmte Geschäftsanwendungen optimiert wird. Das Ergebnis dieses Prozesses ist ein personalisiertes KI-System, das auf die individuellen Herausforderungen der Organisation reagiert.

4. **DeepL, Google Translate**

Beliebte maschinelle Übersetzungssysteme, die dank maschinellem Lernen den Kontext einer Erklärung immer genauer wiedergeben können. Ihr Nachteil ist jedoch die eingeschränkte Offline-Funktionalität und die fehlende vollständige Kontrolle über die Sicherheit der übertragenen Daten. In Verbindung mit lokalen Krisenglossaren (z. B. Wörterbüchern für medizinische, feuerwehrtechnische oder polizeiliche Fachbegriffe) können sie jedoch die Geschwindigkeit und Qualität der Kommunikation in Notfällen erheblich verbessern.

5. **ChatGPT**

LLM (Large Language Model) wird nicht nur für Übersetzungen verwendet, sondern auch zur Überprüfung der Übersetzungsqualität und zur Anpassung von Mitteilungen an die Empfänger. In der Praxis kann ChatGPT semantische Fehler in maschinellen Übersetzungen korrigieren und die Botschaft in Situationen vereinfachen, in denen es auf Verständlichkeit für Personen mit unterschiedlichen Sprachkenntnissen ankommt. Darüber hinaus kann es zur Erstellung von

Zusammenfassungen von Berichten verwendet werden, was die Entscheidungsfindung beschleunigt.

6. **ElevenLabs (Sprachsynthese)**

   Ein Tool zur Generierung natürlich klingender Sprachmeldungen in verschiedenen Sprachen. Im grenzüberschreitenden Krisenmanagement kann es beispielsweise zur schnellen Verbreitung von Alarmmeldungen, Briefings oder Einsatzbefehlen verwendet werden. Dank der Mehrsprachenunterstützung ist es möglich, eine Meldung sofort beispielsweise in Polnisch, Deutsch und Englisch zu erstellen, was die Kohärenz der Maßnahmen der Dienste erhöht.

7. **Kommerzielle Lösungen für Übersetzungen**

   – Deepl Voice: https://www.deepl.com/de/products/voice/deepl-voice-for-meetings,
   – Live Voice: https://livevoice.io/en/ai-voice-translation,
   – Vasco: insb. https://vasco-electronics.de/translator/vasco-translator-e1 und andere mehr.

Die Rolle der künstlichen Intelligenz in der mehrsprachigen Kommunikation kann sich in der operativen Arbeit als entscheidend erweisen, da sie Folgendes bietet:

- kontextbezogene Übersetzung, da sich KI im Gegensatz zu herkömmlichen Systemen nicht auf lexikalische Entsprechungen beschränkt, sondern den situativen Kontext berücksichtigt, was in der Krisenkommunikation unerlässlich ist,

- Reduzierung von Entscheidungsfehlern durch schnelle und genaue Übersetzungen, die das Risiko operativer Missverständnisse verringern,

- Standardisierung von Begriffen, da KI die Erstellung und Pflege von Branchen-Glossaren unterstützen kann und so ein einheitliches Verständnis der Begriffe auf beiden Seiten der Grenze gewährleistet,

- Automatisierung des Informationsflusses, da KI-Tools in Krisenmanagementsysteme integriert werden können, sodass Mitteilungen automatisch übersetzt und verteilt werden,

- Verfügbarkeit in Echtzeit, da letztendlich eine KI-Lösungsarchitektur möglich ist, die einen sofortigen Einsatz auch ohne Netzwerkzugang ermöglicht. Dies ist entscheidend in Situationen, in denen jede Minute über den Erfolg einer Rettungsaktion entscheiden kann.

Die Ergebnisse der Studie zeigen, dass die Rolle der KI in der mehrsprachigen Kommunikation zunimmt – bereits heute nutzen mehr als drei Viertel der Befragten solche Lösungen regelmäßig oder gelegentlich. Der Einsatz von Tools wie PLLuM, Ollama, ChatGPT oder ElevenLabs kann nicht nur die Reaktionszeit verkürzen, sondern auch das Risiko von Fehlern aufgrund von Sprachbarrieren minimieren. In den kommenden Jahren ist zu erwarten, dass KI zu einem integralen Bestandteil grenzüberschreitender Krisenmanagementstrukturen wird, ähnlich wie heute digitale Funksysteme oder gemeinsame Datenaustauschplattformen zum Standard gehören.

Beispiel für den Einsatz von KI-Tools während praktischer Übungen:

1. Erstellung einer Mitteilung in der Ausgangssprache – Vorbereitung des Basistextes mit den wichtigsten operativen Informationen, die an die Dienste oder Teilnehmer der Übung weitergegeben werden sollen,
2. automatische Übersetzung (DeepL) – schnelle Übersetzung der Mitteilung in die Zielsprache unter Beibehaltung des grundlegenden semantischen Kontexts,
3. Korrektur und Anpassung des Inhalts (ChatGPT) – Überprüfung der Übersetzung, Beseitigung potenzieller Ungenauigkeiten und Anpassung der Botschaft an die Situation, die Empfänger und den erforderlichen Kommunikationsstil (z. B. formell, informativ, alarmierend),
4. Sprachsynthese (ElevenLabs) – Auswahl einer geeigneten Stimme und Wiedergabe der Nachricht in Form einer Sprachausgabe, mit der Möglichkeit, Klangfarbe, Tempo oder Intonation anzupassen, damit die Nachricht klar und eindeutig verständlich ist.

2.4. KI bei der Überprüfung von Informationen

Desinformation stellt eine der größten Gefahren im Krisenmanagement dar – sie kann Maßnahmen der Behörden verzögern, das Vertrauen der Bevölkerung untergraben und Chaos unter den Bürgern verursachen. Besonders gefährlich ist die Verbreitung falscher Inhalte in sozialen Medien, wo die Geschwindigkeit der Verbreitung die Möglichkeiten der manuellen Überprüfung übersteigt. In diesem Zusammenhang spielt künstliche Intelligenz eine Schlüsselrolle, indem sie Analyse-, Überwachungs- und Faktenprüfungsprozesse unterstützt. Das Paradoxe daran ist jedoch, dass dieselbe künstliche Intelligenz auch dazu genutzt wird, um diese Fake News in Umlauf zu bringen. Oft können dieselben Tools, die für gute Zwecke entwickelt wurden, auch für schlechte Zwecke missbraucht werden.

Anwendungen von KI-Tools

1. Analyse von Beiträgen in sozialen Medien

- KI kann große Datenmengen in Echtzeit verarbeiten und Inhalte identifizieren, die von offiziellen Krisenmeldungen abweichen.
- **Beispiele für Tools:**
- Hugging Face Transformers – NLP-Modelle zur Sentimentanalyse, Inhaltsklassifizierung und Erkennung sprachlicher Anomalien,
- **CrisisNLP** – Forschungsplattform, die die Analyse von Krisenbeiträgen auf Twitter und deren Klassifizierung (z. B. informativ vs. desinformativ) ermöglicht,
- **Brandwatch / Meltwater** – kommerzielle Medienbeobachtungssysteme, die KI einsetzen, um Trends und Abweichungen von offiziellen Quellen zu verfolgen.

2. **Cross-lingual fact-checking (Vergleich von Inhalten in mehreren Sprachen)**
    - Fehlinformationen verbreiten sich oft grenzüberschreitend, und die Inhalte werden in verschiedene Sprachen übersetzt oder umgeschrieben. KI kann Unstimmigkeiten in den Botschaften automatisch erkennen.
    - Beispiele für Tools:
        - Google Fact Check Tools – ermöglicht die Überprüfung von Inhalten in mehreren Sprachen durch den Abgleich mit einer Datenbank verifizierter Artikel.
        - Meta AI – Sphere – ein Modell, das Wikipedia in mehreren Sprachen durchsucht, um Informationen automatisch zu überprüfen.
        - ML-basierte mehrsprachige Faktenprüfungs-Pipelines – Forschung zu Systemen, die maschinelle Übersetzungen (z. B. DeepL) mit NLP-Modellen zur Analyse der semantischen Konsistenz kombinieren.
3. **Aufdeckung der Verbreitung falscher Narrative auf verschiedenen Plattformen**
    - KI ist in der Lage, sich wiederholende narrative Muster zu erkennen, z. B. dieselben Falschmeldungen, die auf Facebook, Twitter und Telegram veröffentlicht werden.
    - Beispiele für Tools:
        - **PHEME Project –** ein europäisches Projekt, das untersucht, wie sich Gerüchte und Fake News in sozialen Netzwerken verbreiten; es nutzt KI, um Inhalte als „wahr", „falsch" oder „unbestätigt" zu klassifizieren.
        - **Graphika –** ein kommerzielles System, das Netzwerke analysiert und koordinierte Desinformationskampagnen identifiziert.
        - **BRAND24** – ebenfalls eine kommerzielle Lösung zur Überwachung einer Marke im Internet und der Orte, an denen sie erwähnt wird. Das Tool könnte im Zusammenhang mit den Aktivitäten der lokalen Selbstverwaltung und der Identifizierung falscher Informationen eingesetzt werden.
        - **andere Kanäle** – z. B. das Portal Reuters Fack Check oder das polnische Demagog.pl, die aktuelle Ereignisse diskutieren und versuchen, öffentliche Inhalte, insbesondere Kommentare von Politikern, zu überprüfen.

2.5. Sicherheit von KI-Tools

Die Implementierung von KI-Tools im Bereich Krisenmanagement und grenzüberschreitende Kommunikation erfordert besondere Aufmerksamkeit in Bezug auf Sicherheitsfragen. KI kann zwar die Dienste erheblich unterstützen, wird aber gleichzeitig zu einem neuen Angriffsvektor. Unzureichende

Sicherheitsvorkehrungen können zu Manipulationen der Modelle, zur Kompromittierung von Daten oder zum Verlust des Vertrauens in die generierten Inhalte führen. Zu den Gefahren zählen insbesondere

1. **Prompt injection**
    - der Angriff besteht darin, Inhalte in das KI-System einzuführen, die das Modell dazu veranlassen sollen, sein Verhalten in unerwünschter Weise zu ändern.
    - Beispiel: Während Krisenübungen kann der Angreifer eine Nachricht einfügen, die die Dienste in die Irre führt (z. B. indem sie die Bedeutung von medizinischen Begriffen oder Evakuierungsanweisungen verändert).
    - Auswirkungen: unbefugte Handlungen der KI, Generierung falscher Meldungen, Verringerung der Zuverlässigkeit des Systems
2. **Data poisoning**
    - besteht darin, manipulierte Daten gezielt in die Trainingsdatensätze des Modells einzufügen, was sich auf dessen zukünftige Vorhersagen und Ergebnisse auswirkt,
    - Beispiel: In den Datensätzen zu den Standorten von Evakuierungspunkten werden absichtlich falsche Informationen eingefügt, die später von der KI als zuverlässig behandelt werden,
    - Folgen: Verlust der Integrität der Modelle, Risiko falscher operativer Entscheidungen, langfristige Schwächung des Systems
3. **Datenlecks**
    - Risiko, dass vertrauliche Informationen (z. B. Dienstberichte, personenbezogene Daten von Geschädigten, Informationen über kritische Infrastrukturen) bei der Nutzung von Cloud-Modellen an externe Systeme weitergegeben werden,
    - Beispiel: unkontrollierte Nutzung einer öffentlichen Sprachmodell-API, die Daten außerhalb der Verwaltungsinfrastruktur überträgt,
    - Folgen: Verstöße gegen die DSGVO und Datenschutzbestimmungen, Möglichkeit der Nutzung der Informationen für hybride Aktivitäten durch feindliche Akteure

Empfohlene Lösungen:

1. **Hosting von Modellen auf einer von der Verwaltung kontrollierten Infrastruktur (vor Ort)**
    - Die Modelle können lokal trainiert und ausgeführt werden, ohne dass Daten in die öffentliche Cloud übertragen werden müssen.
    - Beispiel: Verwendung von PLLuM als polnisches Sprachmodell, das in einer geschlossenen Infrastruktur funktioniert.

2. **Netzwerksegmentierung und Mikrosegmentierung**
    - Begrenzung der Angriffsfläche durch Trennung der KI-Systeme von anderen Netzwerkkomponenten,
    - Beispiel: Trennung der Server, die KI-Modelle bedienen, von medizinischen oder polizeilichen Meldesystemen.
3. **Verschlüsselung von Daten im Ruhezustand und während der Übertragung**
    - Anwendung von End-to-End-Verschlüsselungsmechanismen in der Kommunikation zwischen den Systemmodulen,
    - Beispiel: Verwendung des TLS 1.3-Standards zur Sicherung der Datenübertragung zwischen Anwendungen, die KI nutzen.
4. **Zero-Trust-Prinzip**
    - Es wird davon ausgegangen, dass keine Komponente des Systems standardmäßig vertrauenswürdig ist – jede Interaktion erfordert eine Authentifizierung und Autorisierung.
    - Beispiel: Jede Authentifizierung von Benutzern und Anwendungen, die die API von KI-Modellen nutzen, mit einer Beschränkung der Berechtigungen auf das erforderliche Minimum.

Zusammenfassung

Die Sicherheit von KI-Tools darf nicht als zusätzliches Element betrachtet werden – sie muss zu einem integralen Bestandteil der Architektur von Systemen zur Unterstützung des Krisenmanagements werden. Nur die Kombination fortschrittlicher Technologien (lokale Modelle, Verschlüsselung, Segmentierung) mit geeigneten organisatorischen Verfahren (Zero Trust, Zugriffskontrolle, Audits) ermöglicht die vollständige und sichere Nutzung des Potenzials der künstlichen Intelligenz in Situationen, in denen die Gesundheit und das Leben der Bürger auf dem Spiel stehen.

1. Einsatz lokaler, sicherer Übersetzungsmodelle

- Sprachmodelle wie PLLuM (Polish Large Language Model) sollten in einer von der öffentlichen Verwaltung kontrollierten Infrastruktur gehostet werden, um die Vertraulichkeit und Integrität der Informationen zu gewährleisten, während man sich für Übersetzungszwecke besser auf spezielle Tools konzentrieren sollte.
- Die Integration von Modellen mit Krisenglossaren (z. B. medizinische, polizeiliche und feuerwehrtechnische Terminologie) gewährleistet eine einheitliche Interpretation von Begriffen und eliminiert das Risiko von Mehrdeutigkeiten.

- Beispiel: Eine lokale Einsatzzentrale kann Berichte polnischer und deutscher Behörden automatisch in Echtzeit übersetzen und dabei die volle Kontrolle über die Datensicherheit behalten.

2. Einrichtung eines KI-basierten Informationsverifizierungszentrums

- Ein solches Zentrum könnte als Analysezentrum fungieren, das KI nutzt, um Inhalte in sozialen Medien zu überwachen, sie mit Faktencheck-Datenbanken (z. B. EU vs Disinfo, Poynter IFCN, Google Fact Check Tools) zu vergleichen und potenzielle Informationsrisiken zu kennzeichnen.

- Die Funktion des sprachübergreifenden Faktenchecks ermöglicht die Überprüfung der Konsistenz von Mitteilungen in mehreren Sprachen, was im Bereich der deutsch-polnischen Zusammenarbeit von entscheidender Bedeutung ist.

- Beispiel: In einer Gesundheitskrise könnte das Zentrum schnell falsche Informationen über Behandlungsmethoden aufspüren und kennzeichnen, bevor sie sich verbreiten können.

3. Schulungen für Verwaltungs- und Dienstangestellte

- Selbst die besten KI-Tools sind ohne entsprechend geschulte Anwender nicht effektiv.

- Schulungen sollten folgende Themen umfassen:
  - Umgang mit KI-Tools,
  - Interpretation der von den Modellen generierten Ergebnisse,
  - Cyberhygiene und digitale Sicherheit (z. B. Schutz vor Prompt Injection, Phishing, Fehlinterpretation von Inhalten),

Beispiel: regelmäßige Workshops für Mitarbeiter von Krisenzentren, Simulationen mit KI und Übungsszenarien zu Desinformationsangriffen

4**. Penetrationstests und Audits von KI-Tools**

- Jedes KI-Tool sollte vor seiner Freigabe für den operativen Einsatz einer Prüfung durch unabhängige Stellen unterzogen werden, und es sollte eine Governance durchgeführt werden, d. h. es sollten Regeln für die Nutzung des Tools festgelegt werden.

- Penetrationstests ermöglichen es, die Widerstandsfähigkeit der Modelle gegen Manipulationen, Versuche der Datenlecks oder Anfälligkeit für Data Poisoning zu überprüfen.

- Audits sollten regelmäßig durchgeführt werden, wobei sich entwickelnde Bedrohungen und Modellaktualisierungen zu berücksichtigen sind.

Beispiel: Audit eines automatischen Übersetzungstools, bei dem überprüft wird, ob das System gegen die Einfügung von Prompts resistent ist, die den Inhalt von Krisenmeldungen verändern könnten.

Ilona BIERNACKA-LIGIĘZA

KAPITEL III. KOMMUNIKATION AN DER GRENZE DER KULTUREN IM ZEITALTER DER DIGITALEN GLOBALISIERUNG

3.1. Einführung

Kommunikation ist seit Jahrhunderten die Grundlage für das Funktionieren von Gesellschaften. Dank ihr ist es möglich, Bedeutungen, Werte und Normen zu vermitteln und soziale Bindungen aufzubauen. Moderne Definitionen betonen ihren komplexen Charakter. Kommunikation umfasst sowohl verbale als auch nonverbale Kanäle wie Gesten, Mimik, Intonation oder physische Distanz.[17].

Laut Paleczny beschränkt sich Kommunikation nicht auf den einfachen Transfer von Informationen, sondern ist ein Prozess der gemeinsamen Konstruktion der sozialen Realität[18]. Das bedeutet, dass Sender und Empfänger nicht nur Inhalte austauschen, sondern diese auch im Lichte des kulturellen Kontexts und ihrer eigenen Erfahrungen interpretieren. In Grenzgebieten, in denen verschiedene Sprachen, Traditionen und Wertesysteme aufeinandertreffen, ist Kommunikation besonders anfällig für Störungen, stellt aber gleichzeitig eine potenzielle Quelle für Innovation und Zusammenarbeit dar.

Die dynamische Entwicklung der digitalen Technologien hat das Gesicht der sozialen Kommunikation zusätzlich verändert. Soziale Medien, Internet-Messenger und Informationsplattformen machen den Informationsaustausch schneller, egalitärer, aber auch schwieriger zu kontrollieren. Wie Castells bemerkt, „basiert Macht im Zeitalter des Internets auf der Fähigkeit, Kommunikation zu gestalten" und damit auch Ereignisse zu interpretieren und ihnen Bedeutung zu verleihen.[19].

In Zeiten einer allgegenwärtigen Informationsgesellschaft, deren Entwicklung eng mit Globalisierungsprozessen verbunden ist, sind Informationen zu einer wichtigen strategischen Ressource geworden.[20] Ihre Erstellung, Verbreitung und Interpretation beeinflussen nicht nur individuelle Entscheidungen von Einzelpersonen in Bezug auf Gesundheit, Arbeit oder Investitionen, sondern auch das Funktionieren von Staaten und regionalen Gemeinschaften.[21] Gleichzeitig hat die dynamische Entwicklung der digitalen Technologien sowohl die Möglichkeiten des schnellen Zugriffs auf Daten als auch die mit ihrer Nutzung verbundenen Risiken erhöht – von Desinformation bis hin zu Cyberangriffen auf kritische Infrastrukturen.[22]

17 J. K. Burgoon, L.K Guerrero, K. Floyd, Nonverbal Communication, Routledge, 2016.

18 T. Paleczny, Komunikacja międzykulturowa w globalizującym się świecie (Interkulturelle Kommunikation in einer globalisierten Welt), [in:] T. Paleczny, M. Banaś (Hrsg.), Dialog na pograniczach kultur (Dialog an den Schnittstellen der Kulturen), Nomos, Kraków 2009, S. 53-75.

19 M. Castells, Communication power, Oxford University Press, Oxford 2009, S. 72.

20 R. Robertson, Globalization: Social theory and global culture, Sage, London 1998.

21 J. W. Seifert, The effects of information technology on governance: A theoretical perspective, Congressional Research Service, Washington, DC, 2002.

22 K. Hafez, The myth of media globalization, Polity Press, Cambridge 2007.

Dank der neuen Medien können die Einwohner in Grenzgebieten wie Słubice - Frankfurt (Oder) oder Gubin - Guben schneller auf Krisensituationen reagieren, soziale Hilfe organisieren und Sprachbarrieren durch automatische Übersetzungen oder zweisprachige Profile von Institutionen überwinden. Gleichzeitig besteht jedoch die Gefahr, dass Unterschiede im Kommunikationsstil von Polen und Deutschen, z. B. in Bezug auf Direktheit oder den Ausdruck von Emotionen, zu Missverständnissen führen können, insbesondere wenn Informationen unter Zeitdruck und hohem Stress verbreitet werden.

3.2. Viele Kulturen – eine gemeinsame Botschaft

Die Wurzeln der interkulturellen Kommunikation liegen in der Anthropologie und Linguistik der zweiten Hälfte des 20. Jahrhunderts. Als ihr Begründer gilt Edward T. Hall, dessen Arbeiten die Unterscheidung zwischen hochkontextuellen und niedrigkontextuellen Kulturen eingeführt haben.[23] In hochkontextuellen Kulturen (z. B. Japan, arabische Länder, bestimmte Kommunikationsaspekte in der polnischen Kultur) hängt die Bedeutung einer Äußerung stark vom situativen Kontext, unausgesprochenen Bedeutungen und der gemeinsamen Geschichte ab. In Kulturen mit geringem Kontext (z. B. Deutschland, skandinavische Länder, USA) ist die Kommunikation direkt, explizit und basiert auf einem eindeutigen Sprachcode.[24] In Kulturen mit hohem Kontext basiert die Kommunikation auf Andeutungen, Symbolen, Traditionen und Konventionen. Worte haben keine vollständige Bedeutung, sondern müssen vom Empfänger durch Kenntnis des Kontexts ergänzt werden. In Kulturen mit geringem Kontext sind Botschaften klar, wörtlich, präzise und weniger von Vermutungen oder zwischenmenschlichen Beziehungen abhängig. Auf der Grundlage dieser Annahme lassen sich Unterschiede in der Krisenkommunikation in Polen und Deutschland feststellen. Polen nehmen häufiger emotionale Botschaften auf, die sich auf Gemeinschaft und Solidarität beziehen, während Deutsche klare Verfahren und eindeutige Anweisungen erwarten. Es ist zu betonen, dass in Krisensituationen eine unklare Kommunikation zu Unsicherheit führen und das Vertrauen in Institutionen auf beiden Seiten der Grenze schwächen kann.

In den 1980er und 1990er Jahren war die Entwicklung der Forschung zur interkulturellen Kommunikation in Europa eng mit den Prozessen der europäischen Integration verbunden. Die Entstehung eines öffentlichen Raums der EU und die zunehmende Mobilität der Bürger erforderten die Schaffung eines theoretischen Rahmens, der die Analyse der Kommunikation in multikulturellen Gesellschaften ermöglichte[25]. In Polen verstärkte sich das Interesse an dieser Thematik nach 1989, als die Öffnung der Grenzen und Migrationen den Kontakt mit anderen Kulturen zu einer alltäglichen Erfahrung machten[26].

Die heutige Dimension der interkulturellen Kommunikation basiert auf zwei grundlegenden Paradigmen: dem Paradigma der kulturellen Unterschiede und dem interaktiven Paradigma[27]. Das erste basiert auf der Annahme, dass jede Kultur relativ stabile Merkmale aufweist, die die Art der Kommunikation bestimmen, während sich das zweite auf den Prozess der Bedeutungsverhandlung im

23 Por. E.T. Hall, The Silent Language, Doubleday & Company Inc., New York 1959 oraz E.T. Hall, Beyond culture, Anchor Books, New York 1976.

24 E.T. Hall, Beyond culture, op. cit., S. 105-116.

25 T. Christiansen, K.E. Jørgensen, A. Wiener (red.), The SAGE handbook of European Union politics, Sage Publications, London 2016.

26 T. Paleczny, Komunikacja międzykulturowa..., op. cit., S. 53-75.

27 M. Byram, Teaching and assessing intercultural communicative competence, Multilingual Matters, Clevedon 1997, S. 13-18.

interkulturellen Kontakt konzentriert. Hofstede[28] vergleicht Länder hinsichtlich Machtdistanz, Individualismus, Unsicherheitsvermeidung, Männlichkeit–Weiblichkeit, Langfristorientierung und Toleranz. Trompenaars und Hampden-Turner[29] konzentrieren sich auf die Hauptachsen kultureller Unterschiede, zu denen sie unter anderem Universalismus-Partikularismus, Neutralität-Emotionalität, Sequenzialität-Synchronicität zählen. Gudykunst[30] konzentriert sich hingegen auf das Phänomen der gegenseitigen Durchdringung von Kulturen und behauptet, dass interkulturelle Kommunikation ein dynamischer Prozess ist, in dem die Teilnehmer ihre Strategien laufend an den Kontext und das Verhalten ihres Partners anpassen (vgl. Tabelle 2).

Tabelle 2. Interkulturelle Kommunikation im deutsch-polnischen Grenzgebiet

Dimension/ Modell	**Polen – Merkmale**	**Deutschland – Merkmale**	**Potenzielle Auswirkungen in einer Krisensituation**
Kommunikationskontext (Hall)	Hoher Kontext, indirekte Kommunikation, Emotionalität	Niedriger Kontext, klare, präzise Kommunikation	Risiko der Fehlinterpretation von Krisenanweisungen
Machtdistanz (Hofstede)	Große Distanz, Akzeptanz der Hierarchie	Kleine Distanz, Erwartung von Transparenz und Konsultation	Konflikte bei der Einführung von Restriktionen von oben
Unsicherheitsvermeidung (Hofstede)	Sehr hoch – Bedürfnis nach klaren Regeln, gleichzeitig Tendenz zur Improvisation	Hoch – Betonung von Verfahren und Planung	Unterschiedliche Reaktionsweisen auf uneindeutige Vorschriften
Universalismus–Partikularismus (Trompenaars)	Tendenz zum Partikularismus, flexible Herangehensweise an Regeln	Starker Universalismus, Einhaltung von Vorschriften	Schwierigkeiten bei der Synchronisierung grenzüberschreitender Maßnahmen
Zukunftsorientierung (GLOBE)	Kurzfristig, reaktiv	Langfristig, strategisch	Mangelnde Kohärenz in der Krisenprognose und -planung

Quelle: eigene Ausarbeitung.

3.3. Kommunikation in Krisenzeiten

Das Krisenmanagement unter globalen Bedrohungen erfordert einen interdisziplinären Ansatz, bei dem die Kommunikation eine zentrale Rolle spielt[31]. Ein effektiver Informationsaustausch zwischen Zentralbehörden, Kommunalverwaltungen, Medien, Nichtregierungsorganisationen und den Bürgern selbst entscheidet darüber, ob es möglich sein wird, Chaos zu begrenzen, Panik zu verhindern und Vertrauen in der Gesellschaft aufzubauen. Dies ist besonders wichtig in Grenzgebieten, in denen sich verschiedene politische, sprachliche und kulturelle Ordnungen überschneiden. Informationen prägen nicht nur die Funktionsweise von Volkswirtschaften, sondern beeinflussen auch grundlegend das soziale

28 G. Hofstede, Culture's consequences: Comparing values, behaviors, institutions and organizations across nations (2nd ed.), Sage Publishing, Thousand Oaks 2001.

29 F. Trompenaars, C. Hampden-Turner, Riding the waves of culture: Understanding diversity in global business (2nd ed.), Nicholas Brealey Publishing, London 1997.

30 W.B. Gudykunst, Bridging differences: Effective intergroup communication (4th ed.), Sage Publications Inc., Thousand Oaks, London, New Delhi 2004.

31 A. Boin, P. Hart, E. Stern, B. Sundelius, The politics of crisis management: Public leadership under pressure (2nd ed.), Cambridge University Press, Cambridge 2017, S. 69-70.

Verhalten, politische Prozesse und interkulturelle Beziehungen. Wie Wnuk-Lipiński[32] feststellt, funktioniert die Globalisierung der Kommunikation wie ein System miteinander verbundener Gefäße: Informationen, die an einem Ort generiert werden, wirken sich fast sofort auf andere Regionen aus, darunter auch auf den Bereich der öffentlichen Sicherheit.

Die Erfahrungen aus der Zeit der Pandemie, des Krieges in der Ukraine oder der Migrationsspannungen bestätigen, dass Krisenkommunikation in einem multikulturellen und grenzüberschreitenden Umfeld nicht nur als technisches Instrument zur Bewältigung von Notfällen betrachtet werden darf. Es handelt sich um einen sozialen Prozess, der in unterschiedlichen kulturellen, sprachlichen und politischen Kontexten verwurzelt ist und nicht nur effiziente Informationskanäle, sondern auch gesellschaftliches Vertrauen, Partizipation und ein angemessenes Maß an Medienkompetenz erfordert[33].

Der Begriff der Krise wird in der Literatur auf vielfältige Weise definiert. Nach Baradyna et al. stellt eine Krise den Höhepunkt einer Krisensituation dar, d. h. den Moment, in dem die Anhäufung von Spannungen, Gefahren und Fehlern zu schwerwiegenden Störungen im Funktionieren des sozialen Systems führt[34]. Tyrała betont, dass Krisensituationen ein unerwünschtes Phänomen sind, da sie ein hohes Risiko für die Verletzung sozialer Bindungen, die Destabilisierung des Wirtschaftslebens und den Verlust des Vertrauens der Bürger in öffentliche Institutionen mit sich bringen[35]. In der Fachliteratur werden zwei grundlegende Modelle für das Kommunikationsmanagement in Krisensituationen unterschieden:

1. Post-reaktives Modell – es sieht eine Reaktion erst nach Auftreten der Krisensymptome vor; es basiert auf hierarchischer Kommunikation (Top-down) und zeichnet sich durch begrenzte Möglichkeiten der Einbindung lokaler Gemeinschaften aus;

2. Pro-reaktives Modell – basiert auf der frühzeitigen Erkennung von Gefahren, der Schaffung von Raum für Dialog und der aktiven Einbeziehung der Bürger in den Krisenmanagementprozess. In diesem Ansatz wird die Gemeinschaft zum Mitgestalter von Lösungen, was den Aufbau von Sozialkapital und Vertrauen fördert.[36].

Tabelle 3. Modelle für das Krisenkommunikationsmanagement

Model	Art der Kommunikation	Rolle der Zentralbehörden	Rolle der lokalen Gemeinschaft	Haupt-Herausforderungen
Post-reaktiv	Hierarchisch, einseitig („von oben nach unten")	Dominierend, zentralisiert	Passiv, Empfänger von Informationen	Verzögerte Reaktion, Informationschaos

32 E. Wnuk-Lipiński, Świat międzyepoki. Globalizacja, demokracja, państwo narodowe (Die Welt zwischen den Epochen. Globalisierung, Demokratie, Nationalstaat), Scholar, Warszawa 2004, S. 23-29.

33 K. Sienkiewicz-Małyjurek, Zarządzanie kryzysowe w administracji publicznej. Teoria i praktyka (Krisenmanagement in der öffentlichen Verwaltung. Theorie und Praxis), Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice 2015.

34 M. Baradyn, Górski, J., & Zalewski, A., Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego (Krisenmanagement im nationalen Sicherheitssystem). Warszawa: Akademia Obrony Narodowej, 2010.

35 P. Tyrała, Zarządzanie kryzysowe: Teoria i praktyka (Krisenmanagement: Theorie und Praxis), Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego, 2001.

36 A. Boin, P. Hart, E. Stern, B. Sundelius, The politics of crisis management, op. cit., S. 49-51.

Model	Art der Kommunikation	Rolle der Zentralbehörden	Rolle der lokalen Gemeinschaft	Haupt-Herausforderungen
Pro-reaktiv	Dialogorientiert, basisorientiert und vernetzt	Koordinierend, unterstützend	Aktiv, partizipativ	Schwierigkeiten beim Aufbau von Vertrauen und Kompetenzen

Quelle: eigene Ausarbeitung auf Grundlage von A. Boin, P. Hart, E. Stern, B. Sundelius, The politics of crisis management: Public leadership under pressure (2. Auflage), Cambridge University Press, Cambridge 2017; T. Paleczny, Komunikacja międzykulturowa..., [in:] T. Paleczny, M. Banaś (Hrsg.), Dialog..., Nomos, Krakau 2009.

Frühere Erfahrungen mit dem Kommunikationsmanagement in einer globalen Krise haben gezeigt, dass beide Modelle in der Praxis parallel funktionierten. Länder wie Polen neigten in der ersten Phase der Covid-19-Krise zum postreaktiven Modell, was zu Informationschaos und einem Vertrauensverlust in der Bevölkerung führte. In Italien, Deutschland und Großbritannien hingegen wurden Elemente des sozialen Dialogs schneller eingeführt, obwohl auch dort Probleme mit der Zentralisierung von Entscheidungen oder der mangelnden Kohärenz der Mitteilungen nicht vermieden werden konnten.

Eine modellhafte Krisenkommunikation ist daher nicht nur eine unpersönliche Verbalisierung von Inhalten, sondern ein sehr komplexes und präzise geplantes Maßnahmenpaket, das in einer Krisensituation ergriffen wird, um die Auswirkungen der Krise zu begrenzen, die Öffentlichkeit zu beruhigen und ihr Zugang zu verlässlichen Informationen zu gewährleisten. Eine Schlüsselrolle in diesem gesamten Prozess spielen natürlich die Medien, die in Krisenzeiten zu einem der wichtigsten Akteure auf der Bühne werden. Laut Grzegorczyk[37] „gibt es keine Krise ohne Medien", da sie den Ereignissen eine bestimmte Interpretation geben, die Themenhierarchie ordnen und die Stimmung in der Gesellschaft prägen. Wenn man sich auf die Besonderheiten der Krisenkommunikation und die Entwicklung entsprechender Standards konzentriert, sollte man ihre wichtigsten Funktionen bei der Erstellung von Mitteilungen in Krisenzeiten erwähnen, darunter:

- Informationsfunktion – schnelle und zuverlässige Übermittlung von Daten über die Gefahr,
- Präventive Funktion – Vorbereitung der Bevölkerung auf mögliche Szenarien, die sich aus Gefahren ergeben,
- Stabilisierende Funktion – Eindämmung von Panik und sozialem Chaos,
- Koordinierende Funktion – Integration der Maßnahmen verschiedener Akteure (Verwaltung, Dienste, NGOs, Medien),
- Bildungsfunktion – Entwicklung der Kompetenzen der Bürger im Umgang mit Informationen,

[37] T. Grzegorczyk, Media w sytuacjach kryzysowych (Medien in Krisensituationen,), Wydawnictwo C.H. Beck, Warszawa 2012.

- Legitimationsfunktion – Aufbau und Aufrechterhaltung des Vertrauens in die öffentlichen Behörden[38].

Von besonderer Bedeutung ist auch die Rolle der Emotionen. Wie Heath und O'Hair betonen, dürfen Mitteilungen von Behörden und Medien in Zeiten der Unsicherheit und des Risikos nicht auf Spekulationen oder emotionaler Sprache basieren, da dies zu einer Eskalation der Ängste führt. Stattdessen sollten sie auf Fakten, klarer Kommunikation und Empathie gegenüber den Empfängern basieren[39]. Daher sollte jede Mitteilung, die während einer Krise an die Öffentlichkeit gerichtet wird, an die aktuelle Phase der Krise, die Rolle, die sie spielen soll, und das Ausmaß der sozialen Spannungen angepasst werden. Die Wahl der Argumente, des Stils und der Ausdrucksmittel ist entscheidend für die Minimierung der negativen Auswirkungen der Krise. Daher ist eine kontinuierliche Zusammenarbeit mit den Medien und ihren Vertretern, sowohl den traditionellen als auch den sozialen, der Weg zum Erfolg.

Die oben genannten grundlegenden Kommunikationsmanagementstrategien haben zu zwei Arten der Krisenkommunikation geführt, die von Praktikern am häufigsten verwendet werden und sowohl der Verwaltungslogik als auch den Bedürfnissen der lokalen Gemeinschaften entsprechen. Diese sind: 1) Einwegkommunikation (basierend auf dem Top-down-Modell) – basiert auf der Annahme, dass die Behörden ein Informationsmonopol haben und diese Informationen einseitig an die Öffentlichkeit weitergeben. Sie zeichnet sich durch schnelle Befehlsausgabe, aber gleichzeitig durch begrenzte Interaktionsmöglichkeiten aus. Diese Art der Kommunikation dominiert in Krisensituationen, in denen die Behörden einseitig Warnmeldungen übermitteln (z. B. „Grenzschließung ab 0:00 Uhr"). 2) Dialogbasierte Kommunikation (basierend auf dem Bottom-up-Modell) – setzt die gleichberechtigte aktive Beteiligung der Einwohner am Informationsaustausch voraus; Konsultationen und Berücksichtigung von Rückmeldungen[40]. Die Bürger können Inhalte mitgestalten, Fragen stellen, während Behörden und Medien als Moderatoren und Partner im Dialog fungieren (z. B. Debatte über Änderungen der Gebühren in der gebührenpflichtigen Parkzone).

Tabelle 4. Typologie der Mitteilungen – Merkmale

Kryterium	Einseitige Kommunikation (reaktiv)	Dialogorientierte Kommunikation (proaktiv)
Kierunek komunikacji	Top-down, einseitig	Zweiwege, vernetz
Rolle des Bürgers	Passiver Empfänger	Aktiver Teilnehmer und Mitgestalter
Dynamik	Reaktion auf Ereignisse nachträglich	Frühwarnung und Zusammenarbeit
Soziales Vertrauen	Gering, Anfälligkeit für Desinformation	Höher, durch Dialog aufgebaut
Hauptrisiko	Informationschaos, Verzögerungen	Schwierigkeiten bei der Koordination, Streuung der Quellen

Quelle: eigene Ausarbeitung.

38 D.L. Sturges, Communicating through crisis: A strategy for organizational survival, "Management Communication Quarterly" Nr. 7(3), 1994, S. 297-316.

39 R.L. Heath, H.D. O'Hair, The Significance of Crisis, op. cit., S. 5-31.

40 M.L. Kent, M. Taylor, Toward a dialogic theory of public relations, "Public Relations Review" Nr. 28(1), 2002, S. 21-37.

In Regionen wie dem deutsch-polnischen Grenzgebiet werden die Herausforderungen im Bereich der Kommunikation noch komplexer. Neben den oben genannten typologischen Standards prallen dort verschiedene sprachliche, administrative und soziale Traditionen aufeinander, was sowohl die Zusammenarbeit fördern als auch Konflikte hervorrufen kann.

Laut Paleczny ist der interkulturelle Dialog eine notwendige Voraussetzung für dauerhafte Sicherheit in Grenzgebieten. Das Unverständnis unterschiedlicher kultureller Codes kann zu Fehlinterpretationen von Krisenmeldungen und damit zu einer Verschärfung von Chaos und Unsicherheit führen[41].

Die interkulturelle Kommunikation in Krisenzeiten hat daher nicht nur eine informative, sondern auch eine integrative Funktion, die die Zusammenarbeit von Gemeinschaften mit unterschiedlichen Traditionen und Erwartungen an die Behörden ermöglicht. Dies erfordert jedoch ausgeprägte interkulturelle Kompetenzen bei Vertretern der Verwaltung, der Medien und sozialer Organisationen[42].

Lokale Selbstverwaltungen sind die erste und den Bürgern am nächsten stehende Ebene der öffentlichen Verwaltung. Sie sind für die Erbringung öffentlicher Dienstleistungen und die Reaktion auf Krisen auf lokaler Ebene zuständig. Die Wirksamkeit ihrer Maßnahmen hängt jedoch von der Qualität der Kommunikation mit den Einwohnern ab[43]. In der Praxis ist in den Grenzregionen häufig eine Dominanz des Transmissionsmodells auf polnischer Seite zu beobachten, wo die von den Behörden veröffentlichten Mitteilungen allgemeiner und normativer Natur sind, während auf deutscher Seite die Kommunalverwaltungen häufiger Konsultationsmechanismen anwenden – z. B. organisieren sie Online-Übertragungen mit Fragen von Bürgern.

Tabelle 5. Krisenkommunikation in den Kommunalverwaltungen Polens und Deutschlands

Aspekt der Kommunikation	**Polen (z.B. Słubice, Gubin, Zgorzelec)**	**Deutschland (z.B. Frankfurt/O, Görlitz, Guben)**	**Auswirkungen in einer Krisensituation**
Kommunikationsstil	Basiert auf Anweisungen und emotionalen Appellen	Basiert auf Verfahren und Konsultationen	Unterschiede in den Erwartungen der Einwohner
Digitale Kanäle	Facebook, Behördenwebsites, SMS vom Woiwoden	Stadtportale, Newsletter, mobile Apps	Fragmentierung der Informationen
Häufigkeit der Mitteilungen	Unregelmäßig, oft eine Reaktion „nach dem Fakt“ (postfaktisch)	Regelmäßige Updates zu festen Zeiten	Höheres Gefühl des Vertrauens auf deutscher Seite
Sprache	Polnisch, sporadisch Deutsch/Englisch	Deutsch + oft zweisprachige polnische Versionen	Sprachbarrieren in Polen, bessere Inklusivität in Deutschland

Quelle: eigene Ausarbeitung.

41 T. Paleczny, Komunikacja międzykulturowa... (Interkulturelle Kommunikation…), op. cit., S. 53-75.

42 M. Byram, Teaching and assessing…, op. cit., S. 13-18; M.W. Lustig, J. Koester, Intercultural competence: Interpersonal communication across cultures (6th ed.), Allyn & Bacon, Boston 2010, S. 24-56.

43 T.R. Aleksandrowicz, Komunikacja kryzysowa w administracji publicznej (Krisenkommunikation in der öffentlichen Verwaltung), Difin, Warszawa 2014; J. Gołębiewski, Zarządzanie kryzysowe w administracji publicznej, Difin, Warszawa 2002.

Tabelle 6. Barrieren in der interkulturellen Kommunikation im Krisenmanagement

Barriere	Polen – Deutschland (Beispiel Grenzregion)	Auswirkungen in einer Krisensituation
Sprachlich	Unterschiede in der polnischen und deutschen Sprache; begrenzte Anzahl zweisprachiger Personen	Verzögerungen bei der Informationsübermittlung, Risiko falscher Interpretationen
Administrativ	Unterschiedliches Rechtssystem und unterschiedliche kommunale Verwaltungsstrukturen	Schwierigkeiten bei der Koordinierung von Rettungsmaßnahmen
Kulturell	Unterschiedliche Kommunikationsstile: Direktheit der Polen vs. größere Formalisierung der Deutschen	Potenzial für Missverständnisse und Konflikte
Sozial	Geringes Vertrauen in die Behörden in Polen vs. höheres Vertrauen in Deutschland	Unterschiedliche Reaktion der Einwohner auf Mitteilungen
Technologisch	Bessere digitale Infrastruktur in Deutschland, Probleme mit dem Internetzugang in polnischen ländlichen Gemeinden	Eingeschränkte Wirksamkeit der digitalen Krisenkommunikation

Quelle: eigene Ausarbeitung auf Grundlage von T. Paleczny, Komunikacja międzykulturowa…, [in:] T. Paleczny, M. Banaś (Hrsg.), Dialog…, Nomos, Krakau 2009; T. Sobera, Profesjonalizacja…, Difin, Warschau 2023.

Vertrauen ist ein wesentlicher Bestandteil einer effektiven Kommunikation in Krisensituationen[44]. Wenn die Zuverlässigkeit von Informationen angezweifelt wird, greifen lokale Gemeinschaften häufiger auf alternative Informationsquellen zurück – oft von geringer inhaltlicher Qualität – als auf Informationen von Institutionen, was besonders in der polnischen Öffentlichkeit deutlich zu beobachten ist. In einer 2021 im deutsch-polnischen Grenzgebiet durchgeführten Studie gaben 62 % der Einwohner von Słubice an, dass sie Informationen aus deutschen Medienquellen mehr vertrauen als denen aus polnischen, während unter den Einwohnern von Frankfurt (Oder) nur 18 % den polnischen Medienmeldungen vertrauten. Darüber hinaus verlassen sich die Polen deutlich häufiger auf inoffizielle Quellen (Familie/Freunde) als auf polnische offizielle Medien (vgl. Tab. 7).

Tabelle 7. Vertrauen in Informationsquellen in Krisensituationen

Informationsquelle	Słubice (%)	Frankfurt/O (%)
Nationale Medien (PL/DE)	38%	72%
Lokale Medien	54%	61%
Soziale Medien (FB, etc.)	47%	49%
Informationen von der Kommune/Stadtverwaltung	42%	68%
Inoffizielle Informationen (Nachbarn, Bekannte)	65%	40%

Quelle: eigene Ausarbeitung.

Die oben genannten Daten zeigen, dass sowohl traditionelle als auch digitale Medien in Krisenmanagementprozessen die Rolle eines „Informationslieferanten" und Katalysators von Spannungen spielen. Wie Grzegorczyk und Cabaj betonen, berichten die Medien nicht nur über Krisen, sondern konstruieren sie auch, indem sie Fakten auswählen, ihnen eine entsprechende Bedeutung

[44] H. Gu, Li L., Trust and the governance of pandemic risk: Lessons from the COVID-19 crisis, "Journal of Chinese Governance" Nr. 5(2), 2020, S. 1-18.

beimessen und sie in einen narrativen Rahmen einbetten[45]. Im digitalen Zeitalter sind neue Möglichkeiten zur Erstellung und Verbreitung von Informationen entstanden.

Zu den beliebtesten Formen der Medienkommunikation zählen:

- eigene Medien (Websites von Behörden, Profile in sozialen Medien), die eine direkte Kommunikation mit den Bürgern ermöglichen,
- soziale Medien (Facebook, Twitter, YouTube, WhatsApp), die einen sofortigen und interaktiven Dialog ermöglichen,
- Bürgermedien und lokale Informationsportale, die die offizielle Darstellung ergänzen, oft aus einer Bottom-up-Perspektive.

Bei der Auswahl des am besten geeigneten Medienkanals, den wir in der aktuellen Krisensituation nutzen, sollte man sich auch auf die Funktion der Kommunikation konzentrieren und sie entsprechend mit der dominierenden Funktion des jeweiligen Mediums in Einklang bringen (vgl. Tab. 8). Die Funktion muss immer auf das Ausmaß der Krise und ihre Auswirkungen auf die lokale Gemeinschaft abgestimmt sein.

Tabelle 8. Funktionen der Medien in Krisensituationen

Funktion	**Traditionelle Medien (TV, Presse, Radio)**	**Digitale und soziale Medien**
Informationsfunktion	**Glaubwürdig**, aber langsamer	**Sofortig**, aber Risiko von Fake News
Bildungsfunktion	Themenschwerpunkte, Experten	Online-Kampagnen, Infografiken, Videos
Koordinierungsfunktion	Mitteilungen der Behörden, Live-Berichterstattung	Schnelle Push-Benachrichtigungen, lokale Gruppen
Integrationsfunktion	Einheitliche nationale Berichterstattung	Schaffung von Online-Gemeinschaften, Diskussionen von der Basis aus (grassroots)
Persuasive / Legitimationsfunktion	Aufbau von Vertrauen in Institutionen	Direkter Kontakt mit lokalen Führungspersonen

Quelle: eigene Ausarbeitung.

Die Entwicklung neuer Kommunikationstechnologien hat zur Entstehung einer digitalen Öffentlichkeit geführt, in der sich der gesellschaftliche Diskurs weitgehend ins Internet verlagert hat. Dieses Phänomen wird manchmal als digitale Agora bezeichnet, in Anlehnung an den klassischen öffentlichen Raum, den Habermas beschrieben hat[46]. Die Digitalisierung hat die Art und Weise, wie Grenzgemeinschaften in Krisensituationen kommunizieren, radikal verändert. Soziale Medien sind zum wichtigsten Kanal für den Informationsaustausch, die Organisation von Hilfsmaßnahmen und die Beobachtung der öffentlichen Stimmung geworden[47]. Die Pandemie hat den Prozess der Digitalisierung des sozialen

45 T. Grzegorczyk, Media w sytuacjach kryzysowych (Medien in Krisensituationen), op. cit.; J. Cabaj, Komunikacja kryzysowa jako narzędzie zarządzania bezpieczeństwem, [in:] M. Kubiak (Hrsg.), Bezpieczeństwo publiczne w warunkach kryzysu, Difin, Warszawa 2015, S. 45-63.

46 J. Habermas, Strukturwandel der Öffentlichkeit, Neuwied: Hermann Luchterhand Verlag, 1962.

47 L. Palen, Online social media in crisis events, [in:] Proceedings of the 5th International Conference on e-Social Science, University of Manchester, Manchester 2008, S. 76-85; C. Fuchs, Social Media: A Critical Introduction (2nd ed.), Sage, London 2017, S. 66-72.

Lebens beschleunigt – Schulen, öffentliche Verwaltung, Wirtschaft und Medien sind in den Online-Raum umgezogen. Infolgedessen sind soziale Medien zum „Informationsmanagementzentrum" in Krisenzeiten geworden, das eine schnelle Verbreitung von Mitteilungen ermöglicht, aber gleichzeitig das Risiko einer „Infodemie" mit sich bringt[48]. Es ist daher festzustellen, dass digitale Medien einerseits eine enorme Unterstützung, andererseits aber auch eine Gefahr für die Krisenkommunikation darstellen (vgl. Tab. 9).

Tabelle 9. Vorteile und Risiken der Digitalisierung der Krisenkommunikation

Aspekt	**Vorteile**	**Risiken**
Geschwindigkeit der Übermittlung	Sofortige Benachrichtigung der Einwohner	Verbreitung von Fake News und Desinformation
Kommunikationskosten	Geringe Kosten im Vergleich zu traditionellen Medien	Abhängigkeit von kommerziellen Plattformen (z.B. Meta, X)
Reichweite	Erreichen einer großen Anzahl von Empfängern	Digitale Ausgrenzung älterer und sozial ausgeschlossener Personen
Interaktivität	Möglichkeit des Dialogs und Feedbacks	Risiko der Polarisierung und von „Informationsblasen"
Transparenz	Öffentlicher Charakter der Übermittlung	Anfälligkeit für Hackerangriffe und Inhaltsmanipulation

Quelle: eigene Ausarbeitung.

Tabelle 10. Nutzung digitaler Medien in der Krisenkommunikation (Polen–Deutschland)

Kommunikationskanal	**Polen (Słubice, Gubin, Zgorzelec)**	**Deutschland (Frankfurt/O, Guben, Görlitz)**
Facebook	Hauptinformationsquelle, spontane Bürgergruppen	Offizielle Behördenseiten, moderierte Gruppen
Internetseiten	Selten aktualisiert, meist Kopien von Regierungsmeldungen	Regelmäßige Aktualisierungen, PL/DE-Sektionen
Mobile Apps	Wenige, keine einheitliche Strategie	Entwickelt (z.B. Katwarn, NINA-App)
Traditionelle Medien online	Lokale Portale, die oft unbestätigte Inhalte vervielfältigen	Regionale Medien mit Krisensektionen
Content-Übersetzungen	Sporadisch, oft von der Basis (Freiwillige)	Systematisch, institutionell

Quelle: eigene Ausarbeitung.

Tabelle 11. Digitale Krisenkommunikation im Sinne von Hall (hoher und niedriger Kontext)

Kommunikationsdimension (nach Hall)	**Mittlerer Kontext (z.B.: Polen)**	**Niedriger Kontext (z.B.: Deutschland)**
Dominierender Kommunikationsstil	Verbindung direkter Elemente mit Uneindeutigkeit; häufige Verwendung von Metaphern und kulturellen Bezügen	Präzise, eindeutige Sprache; Streben nach Klarheit und Vermeidung von Mehrdeutigkeit
Zwischenmenschliche Beziehungen	Bedeutung persönlicher Kontakte, jedoch unter Beibehaltung formaler Rahmen	Formalismus, Distanz, klare Grenzen zwischen Privat- und Berufssphäre

48 European Commission, Tackling COVID-19 disinformation – Getting the facts right (JOIN/2020/8 final), Brussels s2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0008 (Zugang am: 06.10.2025).

Hierarchie und Rolle der Autoritäten	Respekt vor Hierarchie, aber gleichzeitig Neigung zur Verhandlung	Starke Unterordnung unter Regeln und Vorschriften; Autorität des Rechts und der Verfahren
Digitale Kommunikation (Soziale Medien)	Popularität von Facebook und lokalen Foren; Kommunikation oft emotional, geprägt von politischer und gesellschaftlicher Debatte	Hohes Vertrauen in offizielle Online-Kanäle (Websites von Ämtern, mobile Apps wie die NINA-App); Mitteilungen kurz und sachlich
Reaktionen auf Krisen im Netz	Intensive, oft polarisierende Diskussionen; Neigung, offizielle Mitteilungen infrage zu stellen	Größere Neigung, sich den Anweisungen zu unterwerfen; Warten auf offizielle Quellen
Risiko von Desinformation	Hoch – Anfälligkeit für Verschwörungsnarrative, große Rolle inoffizieller Quellen	Niedrig – starke Kultur des Vertrauens in öffentliche Medien und Institutionen

Quelle: eigene Ausarbeitung.

Aus den oben genannten Zusammenfassungen lässt sich eindeutig schließen, dass der Schlüssel zu einem effektiven Krisenkommunikationsmanagement in einer angemessenen Ausbildung der für die Informationsverbreitung verantwortlichen Personen im Bereich der Kommunikationskompetenzen liegt. Die Professionalisierung der Krisenkommunikation, insbesondere im interkulturellen Kontext, erfordert die Entwicklung spezifischer Fähigkeiten. Wie Sobera[49] betont, stehen öffentliche Einrichtungen in Polen nach wie vor vor der Herausforderung, systematische Schulungen im Bereich der strategischen Kommunikation aufzubauen. Zu den wichtigsten Kompetenzen, die einer kontinuierlichen Verbesserung bedürfen, zählen:

- die Fähigkeit zum Informationsmanagement – einschließlich der Nutzung eigener Medien und digitaler Tools,
- kulturelles Bewusstsein – Verständnis für Unterschiede in Sprach- und Kommunikationscodes,
- Empathie und zwischenmenschliche Fähigkeiten – Aufbau von Verständigungsbrücken unter Stress und Unsicherheit,
- Fähigkeit, auf Desinformation zu reagieren – Einsatz von Fact-Checking-Tools und Zusammenarbeit mit Organisationen, die sich mit der Überprüfung von Inhalten befassen.

Schlussfolgerungen und Empfehlungen

Krisenkommunikation und interkulturelle Kommunikation im öffentlichen Raum bilden die Grundlage moderner Sicherheitssysteme. Die Theorie zeigt, dass nur die Integration von Top-down- und Bottom-up-Ansätzen, unterstützt durch digitale Tools und kulturelle Kompetenzen, die Wirksamkeit von Maßnahmen in Krisensituationen in Grenzgebieten wie dem hier diskutierten Fall von Słubice und Frankfurt (Oder) gewährleisten kann.

[49] T. Sobera, Profesjonalizacja komunikowania w sytuacji kryzysowej (Professionalisierung der Kommunikation in Krisensituationen), Difin, Warszawa 2023, S. 158-205.

In Bezug auf die oben genannten Aspekte ist zunächst anzumerken, dass der Prozess der strategischen Kommunikation in Krisensituationen durch folgende Faktoren gestört werden kann: Aufgrund außerordentlicher rechtlicher Maßnahmen, denen nicht genügend Aufmerksamkeit geschenkt wird und die nicht ausreichend praktisch reflektiert werden, kann es zu Kompetenzkonflikten, Uninformiertheit und administrative Hilflosigkeit auftreten können, die oft mit Datenschutzklauseln oder der Notwendigkeit einer „Koordinierung der Maßnahmen auf höherer Ebene" begründet werden.

Zweitens tritt das Problem auch in Situationen auf, in denen mangelnde Vorbereitung und Ressourcen sowie fehlendes Grundwissen sowohl auf Regierungs- als auch auf Kommunalebene in Bezug auf öffentliche Sicherheit und Ordnung zu verwirrenden organisatorischen und rechtlichen Interpretationen oder Versuchen führen, die Verantwortung auf andere Ebenen der Kommunalverwaltung abzuwälzen. Eine solche Strategie des Krisenkommunikationsmanagements im lokalen öffentlichen Raum hat das Chaos nur noch verschlimmert und unnötige Unruhe verursacht, was die Maßnahmen zur Milderung der Auswirkungen der Krise destabilisiert.

Drittens sind die Form und die Art der Informationsverbreitung in Krisenzeiten von großer Bedeutung für die Qualität der Maßnahmen im Rahmen der Informationsstrategie. Besonders gefährlich ist das Problem der Desinformation auf allen Ebenen, das aus der mangelnden Kontrolle über die Berichterstattung und dem Streben nach Sensationslust resultiert. Das zunehmende Misstrauen gegenüber den Informationen, die der Öffentlichkeit vermittelt werden, hat schwerwiegende Folgen. Es kann dazu führen, dass Menschen offizielle Empfehlungen ignorieren und riskante Verhaltensweisen an den Tag legen. Falsche Informationen wirken sich auch negativ auf Institutionen, Gesellschaften und damit auf die wirtschaftliche und finanzielle Lage aus. Daher ist es von entscheidender Bedeutung, eine effektive Kommunikation im lokalen öffentlichen Raum aufzubauen, die auf der Zusammenarbeit zwischen Vertretern von Behörden, Medien und Nichtregierungsorganisationen beruhen sollte. Lokale Gemeinschaften, die im Zeitalter intelligenter Städte und intelligenter Dörfer funktionieren, erwarten die Schaffung von Medienplattformen und Anwendungen, die es ihnen ermöglichen, effizient und effektiv zu arbeiten und schnell auf auftretende Krisensituationen zu reagieren. Diese Plattformen müssen jedoch Inhalte enthalten, die mit kanonischen Werten wie der Meinungsfreiheit und dem Recht auf Zugang zu verlässlichen Informationen im Einklang stehen.

Die oben dargestellte Analyse zeigt einige Schlüsselbereiche auf, die moderne Kommunalverwaltungen bei der Planung einer wirksamen Kommunikationsstrategie berücksichtigen sollten, darunter:

- Behandlung von Informationen als strategische Ressource – in der heutigen Welt sind ihr Schutz und ihre effektive Nutzung zu einer der Grundlagen für die Sicherheit von Staaten und lokalen Gemeinschaften geworden,

- Auswahl der wichtigsten Medienkanäle (unter Berücksichtigung ihrer jeweiligen Funktion) in Krisenzeiten – ohne Medien gibt es keine Krise, denn sie prägen die Berichterstattung und geben den Ereignissen einen Sinn,

- Verbesserung der Kompetenzen im Bereich der interkulturellen Kommunikation – insbesondere in Grenzregionen, wo sprachliche und kulturelle Unterschiede sowohl zu Synergien als auch zu einer Eskalation der Spannungen führen können,

- Bewältigung der Herausforderungen der Digitalisierung – die Entwicklung der sozialen Medien erhöht die Geschwindigkeit und Verfügbarkeit von Informationen, verstärkt aber gleichzeitig das Risiko von Desinformation und sozialer Polarisierung,

- Professionalisierung der Kommunikation – die Wirksamkeit des Krisenmanagements hängt von der Vorbereitung der Mitarbeiter in Verwaltung, Medien und NGOs im Bereich der Kommunikations- und interkulturellen Kompetenzen ab.

Zusammenfassend lässt sich sagen, dass die systematische Entwicklung wirksamer Kommunikationsstandards im lokalen öffentlichen Raum sich sicherlich positiv sowohl auf die Verwaltung der Gemeinde als auch auf die Stärkung der Bürgerbeteiligung auswirken wird[50] (Laajalahti et al. 2016). Die während der Pandemie, der Schließung von Unternehmen, Institutionen und Schulen oder der Einschränkung des Zugangs zu Gesundheitsdienstleistungen gewonnenen Erfahrungen können ignoriert (verschwiegen) oder genutzt werden, um Schlussfolgerungen zu ziehen und Veränderungen einzuleiten. Darüber hinaus sollten die sich wandelnden Standards der Gemeindeverwaltung Anlass für eine vertiefte Diskussion über den Zustand der Selbstverwaltung und die Wirksamkeit der Kommunikation im lokalen öffentlichen Raum sein. Im aktuellen europäischen Staatsmodell ist die lokale Verwaltung für die Erbringung der meisten öffentlichen Dienstleistungen zuständig und als solche der erste Ansprechpartner für die Bürger. Die Zukunft der Bürger und lokalen Gemeinschaften hängt heute von ihrer Effizienz und Handlungsfähigkeit ab. Leider stärken die Maßnahmen der Zentralregierung und der staatlichen Verwaltung nicht immer die Selbstverwaltung. Manchmal schwächt die Anwendung eines Top-down-Modells die Selbstverwaltung systematisch, was die Erfahrungen mit der COVID-19-Pandemie deutlich gezeigt haben. Daher muss überlegt werden, welche Maßnahmen ergriffen werden können und sollten, um den strategischen, gemeinschaftlichen Charakter der Selbstverwaltung wiederherzustellen und ihre finanzielle und entscheidungsbezogene Stabilität zu gewährleisten.

Anhang Nr. 1

Tabelle 12. Hofstedes Kulturdimensionen und Krisenkommunikation (Polen-Deutschland)

Dimension (Hofstede)	**Polen**	**Deutschland**
Machtdistanz	**Groß** – Erwartung deutlicher Kommunikation von oben; Einwohner zählen auf Entscheidungen der Zentralbehörden, sind aber gleichzeitig oft kritisch und misstrauisch gegenüber politischen Eliten. In der digitalen Kommunikation: Dominanz offizieller Mitteilungen, aber parallel aktive Foren und Basisdiskussionen.	**Gering** – Behörden werden als Partner der Bürger betrachtet; die Gesellschaft erwartet Transparenz und die Möglichkeit, online Fragen zu stellen. In der Krisenkommunikation: schnelle Reaktion der Institutionen und hohe Akzeptanz behördlicher Mitteilungen.
Individualismus vs. Kollektivismus	Individualismus mit Elementen lokaler Gemeinschaftlichkeit. Im Netz: aktives Kommentieren, aber oft in der Logik „jeder kommt alleine zurecht“; größere Anfälligkeit für Polarisierung.	Starker Individualismus – Akzent auf die Rechte des Einzelnen und rationale Argumentation. In den digitalen Medien: Dominanz von

[50] A. Laajalahti, J. Hyvärinen, M. Vos, Crisis communication competence in co-producing safety with citizen groups, “Social Sciences” Nr. 5:13, 2016, S. 1-15.

		Experteninhalten und institutionellen Quellen.
Unsicherheitsvermeidung	**Sehr hoch** – Unsicherheit löst Angst aus und begünstigt die schnelle Verbreitung von Gerüchten und Verschwörungstheorien im Internet. In der Krise: Erwartung detaillierter Anweisungen.	**Mäßig** – größere Akzeptanz von Unsicherheit, Vertrauen in Verfahren und Institutionen. Im Netz: Suche nach offiziellen, überprüften Informationen.
Maskulinität vs. Femininität	**Mäßig maskulinistisch** – in der digitalen Kommunikation treten oft politische Kritik, Streitigkeiten und Rivalität um die „Dominanz der Narrative“ auf.	**Hoch maskulinisierte Kultur** – Krisenbotschaften in digitalen Medien sind formal, sachlich und datenbasiert (z.B. Infektionsstatistiken, Regierungsberichte).
Langzeitorientierung	**Eher kurzfristig** – in der Krise dominieren Ad-hoc- und emotionale Reaktionen, und in den sozialen Medien wird oft ein Mangel an sofortigen Maßnahmen kritisiert.	**Langfristig** – Planung, Strategien, Basis auf wissenschaftlichen Daten. Im Netz: langfristige Bildungskampagnen und systematische Kommunikation der Behörden.
Nachgiebigkeit (Indulgence)	**Mäßig** – in der Krise beobachtet man das Abladen von Emotionen im Netz durch Humor (Memes, Satire).	**Niedrig** – es dominieren zurückhaltende, sachliche Mitteilungen; begrenzter Raum für emotionales Abreagieren im öffentlichen Raum.

Tabelle 13. Trompenaars kulturelle Dimensionen und Krisenkommunikation (Polen-Deutschland)

Dimension (Trompenaars)	**Polen**	**Deutschland**
Universalismus vs. Partikularismus	**Starker Partikularismus** – Präferenz für persönliche Beziehungen, Bedeutung von „Bekanntschaften“ in der lokalen Krisenkommunikation; in digitalen Medien oft Misstrauen gegenüber offiziellen Quellen und Suche nach Informationen in lokalen Gruppen (z.B. Foren von Słubice).	**Universalismus** – Betonung einheitlicher Verfahren, gleicher Regeln für alle. In der Online-Krisenkommunikation dominieren klare, offizielle Richtlinien (z.B. Mitteilungen des RKI, Stadtverwaltungen).
Individualismus vs. Gemeinschafts-Kollektivismus	**Gemischt** – in Krisensituationen ist Individualismus sichtbar (eigenständige Suche nach Lösungen), aber in kleineren Orten gibt es eine starke Nachbarschaftssolidarität.	**Individualismus** – die Bürger erwarten eigenständigen Zugang zu zuverlässigen Informationen und die Möglichkeit, die Handlungen der Behörden zu bewerten. Online-Diskussionen werden analytisch und rational geführt.
Neutralität vs. Emotionalität	**Mäßige Emotionalität** – Krisenmitteilungen werden oft emotional kommentiert, Memes und Ironie als eine Form der Entlastung.	**Neutralität** – Krisenkommunikation ist formal, ausgewogen, auf Fakten und statistische Daten ausgerichtet; Emotionen werden in der offiziellen digitalen Kommunikation marginalisiert.
Spezifität vs. Diffusität	**Diffusität** – die Grenzen zwischen der privaten und öffentlichen Sphäre sind fließend; in sozialen Medien werden oft persönliche Erfahrungen im Zusammenhang	**Spezifität** – deutliche Trennung der privaten und öffentlichen Sphäre; Online-Mitteilungen konzentrieren sich auf Fakten und offizielle Daten, seltener auf persönliche Emotionen.

	mit der Krise offengelegt (z.B. Geschichten von Patienten in der Pandemie).	
Leistung vs. Zuschreibung (Rolle/ Funktion/ Status)	**Zuschreibung** – die kommunikative Autorität in der Krise hängt oft von der sozialen Position ab (z.B. Bürgermeister, Pfarrer, lokaler Anführer), und nicht ausschließlich vom Expertenwissen.	**Leistung** – Experten und Spezialisten haben eine größere Bedeutung; Krisenmitteilungen werden durch wissenschaftliche Daten und professionelle Quellen legitimiert.
Zeitorientierung (Sequentiell vs. Synchron)	**Synchron** – Kommunikation in der Krise ist oft chaotisch, wobei politische, soziale und private Themen in digitalen Medien vermischt werden; es fehlt eine eindeutige zeitliche Trennung.	**Sequentiell** – Krisenmitteilungen sind geordnet, werden in bestimmten Abständen gemäß dem Verfahren veröffentlicht; Präferenz für die Schritt-für-Schritt-Logik.

Tabelle 14. Kulturelle Dimensionen von GLOBE und Krisenkommunikation (Polen-Deutschland)

Dimension (GLOBE)	Polen	Deutschland
Unsicherheitsvermeidung	**Groß** – Starkes Bedürfnis nach klaren Richtlinien; der Mangel an präzisen Online-Informationen führt zu Frustration und erhöhter Anfälligkeit für Desinformation.	**Sehr groß** – Präferenz für präzise Verfahren und zuverlässige Quellen (RKI, Gesundheitsministerium). Die Gesellschaft erwartet detaillierte statistische Daten.
Institutionelle Orientierung	**Mäßig** – Starke Erwartungshaltung gegenüber dem Staat, dass er „das Problem löst“, aber geringe Online-Aktivität von der Basis; es dominiert die Kritik an den Behörden in sozialen Medien.	**Groß** – Vertrauen in Institutionen, aktive Nutzung von Regierungs- und Stadtkanälen; die Einwohner befolgen offizielle digitale Mitteilungen häufiger.
Zukunftsorientierung	**Niedriger** – Krisenkommunikation konzentriert sich hauptsächlich auf aktuelle Probleme; langfristige Auswirkungen (z.B. psychologische) werden seltener berücksichtigt.	**Hoch** – Mitteilungen enthalten Prognosen, epidemiologische Modelle, Szenarien zukünftiger Maßnahmen; digitale Medien erfüllen eine Bildungsfunktion.
Ergebnisorientierung	**Mittel** – Lokale Behörden betonen symbolische Handlungen (z.B. Desinfektion von Straßen), weniger konkrete Daten im Netz.	**Hoch** – Krisenkommunikation konzentriert sich auf die Wirksamkeit der Maßnahmen, messbare Ergebnisse (Anzahl der Tests, Betten in Krankenhäusern).
Gemeinschaftsorientierung	**Hoch im gemeinschaftlichen Bereich** – Mitteilungen über Nachbarschaftshilfe, Sammlungen; viele Basisinitiativen im Netz.	**Mäßig** – Institutionelle Hilfe, organisiert durch den Staat und die lokalen Selbstverwaltungen; weniger spontane soziale Initiativen in der digitalen Kommunikation.
Geschlechtergleichheit	**Mittel** – In Krisenmitteilungen dominiert die Stimme männlicher Politiker und Experten, aber die Rolle weiblicher Führungspersonen lokaler NGOs wächst.	**Hoch** – In den digitalen Medien ist die Präsenz von Expertinnen, Ärztinnen, Beamtinnen sichtbar; Kommunikation ist geschlechtergerechter ausbalanciert.
Machtorientierung	**Hoch** – Die Einwohner erwarten, dass lokale und zentrale Behörden entscheiden und informieren; begrenzte Neigung zur eigenständigen Überprüfung von Mitteilungen in digitalen Medien.	**Niedrig** – Die Gesellschaft erwartet Transparenz und partnerschaftliche Behandlung; lokale Behörden führen eine zweiseitige Online-Kommunikation mit den Einwohnern.

Damian FLISAK

KAPITEL IV. NATIONALE UND EUROPÄISCHE RECHTSRAHMEN IM BEREICH CYBERSICHERHEIT UND KI-INSTRUMENTE

4.1. Einführung

Die dynamische Entwicklung der digitalen Technologien führt dazu, dass der Einsatz von KI-Tools im Bereich des Krisenmanagements, einschließlich der Kommunikation zwischen Staaten, zunehmend in Betracht gezogen wird. Um die rechtlichen und praktischen Folgen solcher Lösungen zu bewerten, muss zunächst zwischen KI-Systemen und herkömmlichen Automatisierungstools unterschieden werden. Trotz ihrer Ähnlichkeiten unterscheiden sich ihre Funktionsweise, ihr Autonomiebereich und ihre potenziellen Auswirkungen auf die Rechte des Einzelnen grundlegend, was sich auch in den geltenden Rechtsvorschriften widerspiegelt.

Vor diesem Hintergrund wird der rechtliche Rahmen für die Einführung und den Betrieb von KI-Systemen im Bereich der Krisenkommunikation unter besonderer Berücksichtigung grenzüberschreitender Situationen vorgestellt. Die Analyse umfasst in erster Linie die Rechtsvorschriften der EU – insbesondere die Verordnung 2024/1689 über künstliche Intelligenz (AI Act), Vorschriften zur Cybersicherheit und nationale Vorschriften.

Im weiteren Verlauf des Kapitels werden die wichtigsten rechtlichen Risiken im Zusammenhang mit der Implementierung von KI-Tools in der Krisenkommunikation erörtert. Dabei geht es sowohl um Risiken, die sich aus technischen Fehlern und fehlerhaften rechtlichen Qualifikationen der Systeme ergeben, als auch um mögliche Normenkonflikte, Verletzungen von Grundrechten oder Probleme der Haftung von Behörden und Beamten.

4.2. Künstliche Intelligenz und automatisierte Systeme

Es ist von grundlegender Bedeutung, zwischen KI-Systemen und automatisierten Lösungen richtig zu unterscheiden. Die richtige Einstufung eines Tools bestimmt den rechtlichen Rahmen, während eine falsche Einstufung zu einer Unterbewertung der Anforderungen für den Einsatz von KI-Tools führen kann (mit dem Risiko, dass die zuständige Behörde diesbezüglich Sanktionen verhängt). Aus offensichtlichen Gründen ist eine Überregulierung von Tools, die keine Merkmale künstlicher Intelligenz aufweisen, ebenso unerwünscht.

Gemäß Artikel 3 Absatz 1 des AI Act ist ein KI-System ein maschinelles System, das für den Betrieb mit unterschiedlichem Autonomiegrad ausgelegt ist, sich an die Bedürfnisse des Benutzers anpassen kann und in der Lage ist, auf der Grundlage von Eingabedaten bestimmte Ergebnisse (z. B. Vorhersagen, Inhalte, Empfehlungen, Entscheidungen) zu generieren, die sich auf die Außenwelt auswirken[51].

[51] „'KI-System' bezeichnet ein Maschinensystem, das für den Betrieb mit unterschiedlichem Autonomiegrad nach seiner Implementierung ausgelegt ist und nach seiner Implementierung Anpassungsfähigkeit zeigen kann und das für explizite oder implizite Zwecke – auf der Grundlage der erhaltenen Eingabedaten Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen generiert, die sich auf die physische oder virtuelle Umgebung auswirken können".

Entscheidend für die Identifizierung künstlicher Intelligenz sind vor allem die Fähigkeit zum Schlussfolgern und die Anpassungsfähigkeit. Mit anderen Worten: KI lernt anhand von Daten, aktualisiert ihre interne Struktur und ist in der Lage, Ergebnisse zu generieren, die in ihrem Code nicht direkt vorgesehen sind. Ein traditionelles automatisiertes System funktioniert hingegen anders: Es führt vorab festgelegte, deterministische Regeln vom Typ „wenn-dann" aus, lernt nicht und modelliert keine Realität außerhalb dessen, was in ihm programmiert wurde. Aufgrund dieser bedeutenden Unterschiede ist KI unvergleichlich effektiver, insbesondere bei komplexen Aufgaben. Andererseits sind die von ihr generierten Ergebnisse oft schwer – oder sogar unmöglich – vollständig zu erklären (das sogenannte „Black-Box"-Problem).

Aufgrund ihrer Eigenschaften erfordern KI-Systeme eine menschliche Aufsicht und eine kontinuierliche Überwachung ihrer Funktionsweise. Es wird auch empfohlen, nur begrenztes Vertrauen in die Funktionsweise von KI zu setzen. Nutzer sollten sich nicht übermäßig auf automatische Empfehlungen verlassen oder der trügerischen Überzeugung erliegen, dass intelligente Systeme „unfehlbar" sind (sogenannte KI-Überbewertung, Automatisierungsbias).

In diesem Zusammenhang ist unbedingt auf Artikel 4 des AI Act hinzuweisen, der eine allgemeine Verpflichtung zur Gewährleistung und Aufrechterhaltung eines angemessenen Kompetenzniveaus im Bereich der KI bei den Mitarbeitern des Unternehmens festlegt, das das KI-System einsetzt. Bei der Nutzung eines KI-Systems schreibt die Vorschrift ausdrücklich vor, dass geeignete Maßnahmen zur Gewährleistung eines angemessenen Kompetenzniveaus (KI-Kompetenz) zu ergreifen sind, wobei unter anderem die Ausbildung, Erfahrung und Schulung dieser Personen sowie der Kontext der Nutzung des Systems und die Gruppen, auf die es angewendet wird, zu berücksichtigen sind. Diese Verpflichtung ist dauerhaft, was bedeutet, dass die Kompetenzen mit der Weiterentwicklung der KI-Modelle aufrechterhalten und aktualisiert werden müssen. Unter dem Begriff „KI-Kompetenz" sind sowohl technische Fähigkeiten und Kenntnisse (Verständnis der Funktionsweise des Modells, datenbedingte Einschränkungen, Kenntnis von Notfallszenarien, Orientierung auf dem Markt für KI-Systeme mit der gewünschten Funktionalität usw.) als auch Kenntnisse der regulatorischen Grundlagen zu verstehen. Gerade bei der grenzüberschreitenden Anwendung von KI-Tools sollte das Wissen über die Regulierung auch die Kenntnis der unterschiedlichen Rechtsordnungen auf beiden Seiten der Grenze umfassen. Obwohl der AI Act nicht ausdrücklich die Einrichtung einer speziellen Funktion vorschreibt, wäre es sinnvoll, in der Einheit, die das KI-Tool einsetzt, eine verantwortliche Person zu benennen (ähnlich wie den Datenschutzbeauftragten für den Schutz personenbezogener Daten). Neben der Überwachung der Funktionsweise des KI-Tools sollte diese Person auch für die Verbesserung der KI-Kompetenzen in der gesamten Einheit sorgen.

4.3. Wichtige rechtliche Rahmenbedingungen für KI und Cybersicherheit im Zusammenhang mit der Krisenkommunikation

Grenzüberschreitende Krisensituationen erfordern eine schnelle und koordinierte Kommunikation zwischen den Rettungsdiensten und der öffentlichen Verwaltung Polens und Deutschlands. Moderne KI-Tools können in diesem Bereich eine unschätzbare Unterstützung bieten (von der Klassifizierung von Notrufen und der Vorhersage von Ereignisentwicklungen über die automatische Generierung bis hin zur Übersetzung von Mitteilungen für die Bevölkerung).

Der Einsatz von KI-Tools in einem so sensiblen Bereich wie dem Krisenmanagement muss jedoch innerhalb eines streng definierten rechtlichen Rahmens erfolgen. Der zentrale Bezugspunkt in regulatorischer Hinsicht ist das Gesetz über künstliche Intelligenz (AI Act), dessen Bestimmungen einheitliche Standards für alle Mitgliedstaaten, also auch für Polen und Deutschland, schaffen. Von Bedeutung sind auch eine Reihe weiterer EU- und nationaler Vorschriften, die im Folgenden näher erläutert werden. Schließlich sind auch bilaterale polnisch-deutsche Abkommen über gegenseitige Hilfe und grenzüberschreitende Zusammenarbeit von Bedeutung.

All diesen Rechtsakten ist gemeinsam, dass sie sicherstellen sollen, dass künstliche Intelligenz auf sichere, transparente und grundrechtskonforme Weise eingesetzt wird und gleichzeitig eine schnelle und wirksame Kommunikation in Notfällen ermöglicht.

a) Verordnung über künstliche Intelligenz (AI Act)

In der grenzüberschreitenden Krisenkommunikation im deutsch-polnischen Grenzgebiet unterliegt der Einsatz von KI-Tools den einheitlichen Regeln des KI-Gesetzes, das am 1. August 2024 in Kraft getreten ist (mit vollständiger Anwendung ab August 2026). Das bedeutet, dass auch öffentliche Einrichtungen und Infrastrukturbetreiber auf beiden Seiten der Oder KI-Systeme nach denselben Anforderungen nutzen müssen.

Bei der Kategorisierung von KI-Systemen verfolgt der AI Act einen risikobasierten Ansatz in Bezug auf die Rechte und Freiheiten des Menschen. Je nach Risikograd werden KI-Anwendungen in mehrere Gruppen unterteilt: verbotene Praktiken, Hochrisiko-KI-Systeme und andere Systeme, für die Mindestanforderungen gelten.

Zu den verbotenen Praktiken gehören Lösungen, deren Wesen mit dem Schutz der wichtigsten Werte unvereinbar ist. Zu dieser Gruppe gehören: Manipulationstechniken, einschließlich subliminale (unbewusste) Beeinflussung von Menschen; Ausnutzung der besonderen Anfälligkeit bestimmter Gruppen (z. B. aufgrund ihres Alters oder einer Behinderung) in einer Weise, die ihre Entscheidungen verzerrt; Social Scoring durch öffentliche Behörden (d. h. die systematische Bewertung von Menschen, um Entscheidungen über sie zu treffen); biometrische Kategorisierung zum Zwecke der Ableitung sensibler Merkmale (z. B. politische Ansichten, Religion oder sexuelle Orientierung); Erstellung von Datenbanken zur Gesichtserkennung durch massenhaftes Scraping von Bildern aus dem Internet sowie – vorbehaltlich eng gefasster Ausnahmen – ferngesteuerte biometrische „Live"-Identifizierung im öffentlichen Raum durch Strafverfolgungsbehörden. Die Verordnung schließt auch die Erkennung von Emotionen (am Arbeitsplatz und im Bildungsbereich) aus, um auf dieser Grundlage Schlussfolgerungen zu ziehen. In der Praxis bedeutet dies, dass in Krisenkommunikationsprojekten KI-basierte Lösungen, die auf der Liste der verbotenen Praktiken stehen, kategorisch ausgeschlossen werden müssen.

Eine weitere Kategorie sind risikoreiche KI-Systeme, d. h. solche, die erhebliche Auswirkungen auf die Gesundheit, Sicherheit oder Rechte von Personen haben können. Das KI-Gesetz identifiziert eine umfangreiche Gruppe solcher KI-Systeme. Zur Klarstellung: Diese Systeme sind nicht verboten, unterliegen jedoch strengen Anforderungen in vielen Bereichen ihrer Funktionsweise, insbesondere in Bezug auf Risikomanagement, Qualität der Trainingsdaten, Dokumentation, Überwachung und (in einigen Fällen) Registrierung. Die zu dieser Gruppe gehörenden KI-Systeme sind im Wesentlichen in Anhang III des KI-Gesetzes aufgeführt. Dazu gehören unter anderem biometrische Lösungen; Instrumente zur Unterstützung der Verwaltung kritischer Infrastrukturen, deren Ausfall die Gesundheit

und Sicherheit gefährden könnte; Systeme, die in der allgemeinen und beruflichen Bildung eingesetzt werden, wenn sie über den Zugang zu Bildung entscheiden; Systeme, die in der Beschäftigung und im Personalmanagement eingesetzt werden, einschließlich Rekrutierung, Leistungsbewertung und Beförderung; Technologien, die den Zugang zu grundlegenden privaten und öffentlichen Dienstleistungen, einschließlich Sozial- und Finanzdienstleistungen, beeinflussen; Systeme, die bei der Strafverfolgung und Grenzkontrolle eingesetzt werden; sowie Instrumente, die in der Justiz und in demokratischen Prozessen eingesetzt werden.

In der Realität der Krisenkommunikation und der deutsch-polnischen Grenzregion kann die Einstufung als hochriskante KI-Systeme insbesondere Module betreffen, die der Triage oder Klassifizierung von Notrufen dienen, aber auch die Unterstützung der Einsatzplanung von Rettungskräften und -mitteln, Elemente des Managements kritischer Infrastrukturen (Energie, Wasser, Kommunikation), ausgewählte Anwendungen in den Bereichen Strafverfolgung, Migration und Grenzkontrolle sowie – sofern gesetzlich zulässig – Biometrie. Dies würde die Notwendigkeit einer vollständigen Einhaltung des KI-Gesetzes mit sich bringen. Das System müsste dann einem Risikomanagement und einer Datenkontrolle (einschließlich Qualitäts- und Repräsentativitätskontrolle) unterliegen, über eine vollständige technische Dokumentation und eine Ereignisprotokollierungsfunktion verfügen. Darüber hinaus sollte es die Anforderungen an Genauigkeit, Ausfallsicherheit und Cybersicherheit erfüllen und einer Konformitätsbewertung unterzogen werden. Auf Seiten des Nutzers kommen die bereits oben genannten Verpflichtungen hinzu, eine tatsächliche menschliche Aufsicht durch geschulte Personen sicherzustellen, den Betrieb laufend zu überwachen und schwerwiegende Vorfälle zu melden.

Die übrigen Systeme, die weder unter das Verbot fallen noch zur Kategorie der hohen Risiken gehören, unterliegen minimalen Auflagen. Der AI Act schreibt in bestimmten Fällen weit gefasste Verpflichtungen zur Transparenz der Kommunikation vor. Das bedeutet, dass der Nutzer eines KI-Systems darüber informiert werden muss, dass er mit einer KI interagiert, und dass synthetisch generierte oder durch KI-Systeme veränderte Inhalte (hier geht es um Inhalte jeglicher Art: Text, Bild, Audio, Video) entsprechend gekennzeichnet und als solche erkennbar sein sollten. Im Hinblick auf das Thema Krisenkommunikation muss die Verbreitung von Informationen über Krisenereignisse (z. B. Evakuierungswarnungen, Meldungen über Verkehrsunterbrechungen an Grenzübergängen, Hochwasserwarnungen) diese Anforderungen erfüllen.

Zusammenfassend lässt sich sagen, dass Bei der Einführung von KI in die grenzüberschreitende Krisenkommunikation muss überprüft werden, ob der Einsatz des KI-Tools überhaupt zulässig ist (d. h. ob es sich nicht um eine verbotene Praxis handelt), ob es als hochriskant einzustufen ist und ob das jeweilige Tool über Mechanismen zur Gewährleistung der Transparenz für alle Informationskanäle verfügt.

b) Umsetzung des AI Act in Polen und Deutschland

Obwohl es sich bei dem AI Act um eine Verordnung handelt und somit ein Rechtsakt, der in den EU-Mitgliedstaaten unmittelbar gilt, müssen diese Maßnahmen zur Umsetzung der Bestimmungen der Verordnung ergreifen: von der Benennung der Aufsichts- und Zertifizierungsbehörden für den Markt für KI-Systeme über die Einführung eines Sanktionssystems für die Nichteinhaltung der auferlegten Verpflichtungen bis hin zu nationalen Rechtsbehelfsverfahren oder Verfahren zur Förderung von Innovation.

Der aktuelle Entwurf des polnischen Gesetzes[52] sieht die Einrichtung einer Aufsichtsbehörde (Kommission für die Entwicklung und Sicherheit künstlicher Intelligenz) vor und überträgt dem für die Informatisierung zuständigen Minister die Zuständigkeit für die Ausarbeitung der erforderlichen Verfahren zur Bewertung der Stellen, die die Rechtmäßigkeit der Einführung von Hochrisikosystemen beurteilen. Darüber hinaus präzisiert der Entwurf das Verfahren bei Verstößen und die Regeln für Rechtsbehelfe und regelt Sofortmaßnahmen (z. B. die Anordnung, das System im Falle einer unmittelbaren Gefahr auszusetzen oder zurückzuziehen).

Deutschland setzt den AI Act durch einen Gesetzentwurf um, der vom Bundesministerium für Digitales und Staatsmodernisierung (BMDS) ausgearbeitet wurde[53]. Eine zentrale Rolle bei der Marktüberwachung und Zertifizierung soll die seit vielen Jahren bestehende Bundesnetzagentur (BNetzA) übernehmen, die bisher für die Einhaltung der Regeln des fairen Wettbewerbs auf den Märkten für Strom, Gas, Telekommunikation, Post und Schienenverkehr zuständig war. Es ist geplant, innerhalb der Behörde spezielle Einheiten für sensible Bereiche einzurichten, z. B. die Unabhängige KI-Marktüberwachungskammer (UKIM), die für die Themen Biometrie, Migration und Strafverfolgung zuständig ist.

c) Cybersicherheit

Im Bereich der technischen Sicherheit ist die NIS2-Richtlinie der Bezugspunkt. Sie bezieht sich auf den Bereich der elektronischen Kommunikation und der digitalen Infrastruktur, führt einen Katalog von Risikomanagementmaßnahmen (u. a. Betriebskontinuität, Sicherheit der Lieferkette, Tests, Protokollierung, Verschlüsselung) sowie Fristen für die Meldung von Vorfällen ein. Die Richtlinie legt mehrere Hauptpflichten fest. Auf Ebene der Mitgliedstaaten muss jedes Land eine nationale Strategie für digitale Sicherheit verabschieden, zuständige Behörden und Krisenmanagementbehörden benennen, eine zentrale Kontaktstelle benennen und Computer-Sicherheitsvorfall-Reaktionsteams (CSIRT) einrichten und unterhalten. Kritische und wichtige Akteure (d. h. Organisationen, die in den in den Anhängen der Richtlinie genannten Sektoren tätig sind, z. B. Energie, Verkehr, Gesundheit, öffentliche Verwaltung, digitale Dienste) müssen Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit umsetzen und ihre Meldepflichten für Vorfälle innerhalb bestimmter Fristen erfüllen. Darüber hinaus müssen die Mitgliedstaaten und die betroffenen Unternehmen den Austausch von Daten über Bedrohungen und Vorfälle im Rahmen von CSIRT-Netzwerken, Kontaktstellen und Mechanismen der Zusammenarbeit auf EU-Ebene organisieren und unterstützen. Darüber hinaus sorgen die EU-Mitgliedstaaten für ein wirksames System von Kontrollen, Inspektionen und Sanktionen, um die Anwendung der Anforderungen der Richtlinie gegenüber den unter ihren Anwendungsbereich fallenden Stellen durchzusetzen. Obwohl die Frist für die Umsetzung der Richtlinie im Oktober 2024 abgelaufen ist, wurde sie weder in Polen noch in Deutschland umgesetzt.

---

52 Projekt ustawy o systemach sztucznej inteligencji (Entwurf eines Gesetzes über Systeme der künstlichen Intelligenz), 02.10.2025, https://legislacja.gov.pl/projekt/12390551/katalog/13087932#13087932 (Zugang: 06.10.2025).

53 Vgl. Gesetzesentwurf: Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (Gesetz zur Durchführung der KI-Verordnung), https://bmds.bund.de/fileadmin/BMDS/Dokumente/Gesetzesvorhaben/CDR_Anlage1-250911_RefE_KIVO-Durchf%C3%BChrungsgesetz_Entwurf_barrierefrei.pdf (Zugang: 06.10.2025).

Ergänzt wird die NIS2-Richtlinie durch Verordnungen zur Gewährleistung eines angemessenen Cybersicherheitsniveaus von Produkten mit digitalen Komponenten (Cyber Resilience Act)[54] und deren Zertifizierung (Cybersecurity Act)[55].

Anforderungen hinsichtlich der digitalen Sicherheit ergeben sich auch aus dem AI Act selbst. Die Verordnung verpflichtet Anbieter und Betreiber von Systemen der künstlichen Intelligenz, insbesondere jenen, die als Hochrisikosysteme eingestuft werden, deren Robustheit, Widerstandsfähigkeit und Cybersicherheit (robustness, resilience, cyber security) über den gesamten Lebenszyklus des Systems hinweg zu gewährleisten. Das bedeutet die Notwendigkeit, Lösungen zu entwerfen und umzusetzen, die resistent gegen Manipulationen, Angriffe und Störungen sind, Sicherheitstests durchzuführen, Vorfälle zu protokollieren sowie den Betrieb des Systems ständig zu überwachen.

d) Bilaterale Abkommen und Kooperationsmechanismen zwischen Polen und Deutschland

Die Grundlage für die Zusammenarbeit zwischen Polen und Deutschland im Bereich Krisenmanagement bilden bilaterale Abkommen, die den rechtlichen Rahmen für die gegenseitige Hilfe bei Katastrophen und Naturkatastrophen bilden. Das wichtigste Dokument ist nach wie vor das Abkommen zwischen beiden Ländern aus dem Jahr 1997 über die gegenseitige Hilfe bei Katastrophen, Naturkatastrophen oder anderen schweren Unfällen. Es legt unter anderem die Verfahren für die Beantragung von Hilfe, die Regeln für den Grenzübertritt von Rettungskräften, die Anerkennung ihrer Befugnisse und die Kostenerstattung fest und benennt zentrale Kontaktstellen: in Polen den Minister für Inneres und Verwaltung und in Deutschland das Bundesministerium des Innern (im Falle Brandenburgs das Ministerium für Inneres). Ergänzt wird dies durch regionale Abkommen, darunter das für das Grenzgebiet wichtige polnisch-brandenburgische Abkommen über gegenseitige Hilfe bei Katastrophen, Naturkatastrophen und anderen schweren Unfällen aus dem Jahr 2002. Das Abkommen vereinfacht grenzüberschreitende Verfahren, z. B. ermöglicht es der Feuerwehr, dem Rettungsdienst und anderen Diensten, im Notfall schnell die Grenze zu überqueren, legt regionale Kontaktstellen fest, sieht gemeinsame Übungen und Schulungen sowie den Austausch von Gefahrenwarnungen und die Abstimmung von Mitteilungen vor.

Grundlage für die oben genannten Rechtsakte ist der Vertrag zwischen der Republik Polen und der Bundesrepublik Deutschland über gute Nachbarschaft und freundschaftliche Zusammenarbeit aus dem Jahr 1991, dessen Artikel 12 beide Staaten dazu aufforderte, eine partnerschaftliche Zusammenarbeit insbesondere im Grenzgebiet zu entwickeln[56].

Zusammenfassung

54 Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), (Zugang: 06.10.2025).

55 VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), (Zugang am: 06.10.2025).

56 Vertrag zwischen der Bundesrepublik Deutschland und der Republik Polen über gute Nachbarschaft und freundschaftliche Zusammenarbeit., GBl. 1992 Nr. 14, Pos. 56.

Der Einsatz künstlicher Intelligenz in der grenzüberschreitenden Krisenkommunikation an der Grenze zwischen Polen und Deutschland birgt sowohl enorme Chancen als auch Herausforderungen. KI kann die Informationsverteilung erheblich verbessern, eine schnellere Reaktion auf Gefahren gewährleisten und die Koordination der Rettungsdienste auf beiden Seiten der Grenze verbessern. Gleichzeitig muss dies in strikter Übereinstimmung mit dem EU-Rechtsrahmen – insbesondere dem AI Act und den Vorschriften zur Cybersicherheit – sowie im Rahmen bestehender bilateraler Abkommen und regionaler Kooperationsstrukturen erfolgen. Bei der Einführung von KI-Tools für die Krisenkommunikation müssen Transparenz, Sicherheit und die Aufrechterhaltung der menschlichen Kontrolle gewährleistet sein. Nur dann kann das Potenzial der Technologie voll ausgeschöpft werden, während gleichzeitig die Rechte der Bürger gewahrt und das gegenseitige Vertrauen beider Länder im Bereich des Notfallmanagements gestärkt werden.

Risiken im Zusammenhang mit dem Einsatz künstlicher Intelligenz in Krisenkommunikationssysteme an der Grenze

Der Einsatz künstlicher Intelligenz in Krisenkommunikationssysteme bringt nicht nur offensichtliche Vorteile mit sich, sondern auch erhebliche rechtliche Risiken. Zu den größten Herausforderungen zählen potenzielle Rechtsverstöße aufgrund von Fehlern oder Missbrauch der KI, Schwierigkeiten bei der Qualifizierung von KI-Systemen oder Gefahren für die Grundrechte der Bürger. Problematisch könnte auch der Konflikt zwischen polnischen und deutschen Rechtsnormen sein.

a) Rechtliche Risiken

Der Einsatz von KI in der Krisenkommunikation kann zu Verstößen gegen zahlreiche Rechtsordnungen führen. Insbesondere besteht die Gefahr der Verletzung von Persönlichkeitsrechten, beispielsweise wenn ein KI-System eine Nachricht oder ein Bild generiert, das eine Person in unzulässiger Weise darstellt und damit deren Privatsphäre, guten Ruf oder Würde verletzt. Ein weiteres ernstes Problem kann die illegale Verwendung urheberrechtlich geschützter Inhalte sein, wenn das KI-System Elemente aus den Trainingsdaten reproduziert. Eine weitere erhebliche Gefahr ist die Verletzung der Vertraulichkeit: Systeme, die Notrufe verarbeiten, können sensible Informationen wie medizinische Daten oder Adressen von Evakuierten offenlegen, was unter anderem gegen die Vorschriften zum Schutz personenbezogener Daten verstoßen würde.

Ein wesentliches Risiko bei der grenzüberschreitenden Nutzung von KI in der Krisenkommunikation ist die Möglichkeit von Datenlecks und deren sekundäre Nutzung durch Tool-Anbieter oder Dritte. Diese Gefahr besteht auch dann, wenn die vertraglichen Nutzungsbedingungen eines bestimmten KI-Systems garantieren, dass die Daten nicht für andere Zwecke verwendet oder verarbeitet werden. In der Praxis bedeutet dies das Risiko der Offenlegung sensibler Informationen, die sowohl die betroffenen Personen als auch die Sicherheitsverfahren betreffen.

b) Fehler der KI-Systeme

Eine Fehlfunktion des Algorithmus, der für die Auswahl oder Priorisierung von Alarmmeldungen zuständig ist, kann zu einer fehlerhaften Klassifizierung von Ereignissen führen. Ein schlecht trainiertes System, das mit algorithmischen Vorurteilen (Bias) belastet ist, kann ein weniger dringendes Ereignis als vorrangig einstufen, was zu einer fehlerhaften Einsatzleitung und einer realen Gefahr für Leben oder Gesundheit führen könnte. Aus rechtlicher Sicht wirft dies die Frage der Haftung für unterlassene oder

verspätete Hilfe auf, sei es seitens des Anwenders des KI-Systems, des Anbieters dieses Systems oder anderer Akteure, die an der Wertschöpfungskette von KI-Systemen beteiligt sind.

Da weder das polnische noch das deutsche Recht besondere Vorschriften für Schäden enthält, die durch KI-Systeme verursacht werden, gelten die allgemeinen Regeln der deliktischen und vertraglichen Haftung, die in dem jeweiligen Land gelten. Es ist anzumerken, dass die Europäische Kommission Anfang 2025 den Entwurf einer Richtlinie über die Haftung für KI (AI Liability Directive) zurückgezogen hat, wodurch den Geschädigten wichtige Erleichterungen bei der Geltendmachung von Schadensersatzansprüchen (z. B. durch die Einführung bestimmter Vermutungen) genommen wurden. Es ist davon auszugehen, dass die Geltendmachung von Schadensersatzansprüchen auf der Grundlage allgemeiner Vorschriften nicht einfach sein wird, da die traditionellen Regelungen nicht an die Realitäten der Funktionsweise von KI-Tools angepasst sind. Daher ist es von entscheidender Bedeutung, sich in Verträgen mit Anbietern angemessen abzusichern (z. B. durch Entschädigungsklauseln) und entsprechende Versicherungen abzuschließen.

c) Fehlerhafte Qualifizierung von KI-Systemen

Eine falsche Einstufung eines KI-Tools birgt erhebliche rechtliche und praktische Risiken. Auf der Grundlage des AI Act kann die fehlerhafte Einstufung eines Systems mit hohem Risiko als System mit geringem oder begrenztem Risiko dazu führen, dass eine Reihe der oben genannten Verpflichtungen nicht erfüllt werden. Infolgedessen werden nicht nur die regulatorischen Anforderungen verletzt, sondern auch die Grundrechte der Nutzer und der Personen, deren Daten verarbeitet werden. Im Lichte der NIS2-Richtlinie kann die falsche Einstufung eines Systems als nicht unter die digitalen Sicherheitsverpflichtungen fallend wiederum dazu führen, dass keine geeigneten organisatorischen und technischen Maßnahmen umgesetzt werden, die Meldepflicht für Vorfälle nicht erfüllt wird und die Widerstandsfähigkeit kritischer Infrastrukturen geschwächt wird. Da sich beide Rechtsordnungen gegenseitig ergänzen (eine fehlerhafte Einstufung des Systems kann gleichzeitig einen Verstoß gegen die Verpflichtungen aus dem AI Act und die Verpflichtungen im Bereich der Cyberresilienz gemäß NIS2 bedeuten), ist eine Kumulierung der in beiden Rechtsvorschriften vorgesehenen Sanktionen möglich.

d) Konflikte zwischen Rechtsnormen

In grenzüberschreitenden Systemen kann es zu Konflikten zwischen polnischem und deutschem Recht kommen. Obwohl das EU-Recht die Vorschriften weitgehend harmonisiert, bestehen weiterhin Unterschiede (z. B. hinsichtlich der Anonymisierung personenbezogener Daten). Ein weiterer Bereich, in dem es zu Konflikten kommen kann, ist der Schutz vor Desinformation: In Deutschland verpflichtet das verfassungsrechtliche Richtigkeitsgebot Beamte zu einer besonderen Verantwortung für die Freigabe von Mitteilungen, selbst wenn diese von KI generiert wurden.

e) Gefahren für die Grundrechte

Viele nationale Rechtsvorschriften, aber auch der AI Act betonen die Notwendigkeit der Achtung der Grundrechte, einschließlich des Rechts auf Privatsphäre, des Datenschutzes, des Grundsatzes der Nichtdiskriminierung und des Rechts auf zuverlässige Informationen. In Krisensituationen kann die Erhebung großer Datenmengen (z. B. Standortdaten von Mobiltelefonen) durch die jeweilige Krisensituation gerechtfertigt sein, gleichzeitig aber auch das Risiko von Missbrauch bergen. Ein

Problem kann beispielsweise die Möglichkeit der Diskriminierung durch fehlerhaft funktionierende Algorithmen sein, z. B. durch die Zuweisung schlechterer Evakuierungsbedingungen für Migranten oder Personen, die die jeweilige Sprache nicht beherrschen. Ebenso wichtig ist das Bewusstsein für das Risiko von Desinformation: KI-Systeme können Mitteilungen in einer Weise verändern, die die Realität verzerrt und das Recht der Bürger auf vollständige Information einschränkt.

f) Unterschiede im Krisenmanagement

Eine gewisse Risikoquelle in der grenzüberschreitenden Krisenkommunikation kann das unterschiedliche Modell der Notfallbewältigung in Polen und Deutschland sein. In Polen gilt ein stark zentralisiertes System, in dem das Regierungszentrum für Sicherheit zusammen mit dem Ministerium für Inneres und Verwaltung eine wesentliche Rolle spielt, da sie den Informationsfluss koordinieren und über den Inhalt der Mitteilungen entscheiden. In Deutschland hingegen wurde ein dezentraler Ansatz gewählt. Die Verantwortung für das Krisenmanagement ist verteilt und basiert auf dem Subsidiaritätsprinzip sowie auf Bundes- und Landeskompetenzen, wobei grundsätzlich die Bundesländer die führende Rolle spielen. In lokalen Krisensituationen übernehmen die Landräte und Bürgermeister die Leitung der Krisenmaßnahmen. Diese Asymmetrie kann zu einem Risiko der zeitlichen oder inhaltlichen Nicht-Synchronisation von Mitteilungen, zu widersprüchlichen Entscheidungen oder zu Schwierigkeiten bei der Zuweisung der Verantwortung für fehlerhafte oder verspätete Mitteilungen führen. Darüber hinaus können Probleme mit der Interoperabilität von KI-Tools auftreten, die unter unterschiedlichen administrativen Rahmenbedingungen entwickelt wurden. Ohne klar definierte Koordinierungsmechanismen können KI-Systeme daher die Krisenkommunikation im Grenzgebiet nicht nur nicht verbessern, sondern sogar erschweren.

g) Verantwortung der Verwaltungsangestellten

Der Einsatz von KI-Tools in der Krisenkommunikation birgt nicht nur technische und rechtliche Risiken, sondern auch Haftungsrisiken für Beamte, die die Umsetzung überwachen und Entscheidungen über den Einsatz solcher Systeme treffen.

In Polen gilt der Grundsatz, dass für Schäden gegenüber Bürgern der Staat oder die kommunale Gebietskörperschaft haftet, während der Beamte disziplinarisch, finanziell (Regress) und in Ausnahmefällen auch strafrechtlich haftbar gemacht werden kann (wenn er vorsätzlich oder grob fahrlässig gehandelt hat). In Deutschland gilt das Prinzip der Amtshaftung, wonach der Staat gegenüber dem Bürger haftet und ein Regress gegen den Beamten nur bei Vorsatz oder grober Fahrlässigkeit möglich ist. Beamte unterliegen außerdem strengen dienstrechtlichen Pflichten, die sich aus dem Beamtenrecht ergeben, darunter dem Grundsatz der Loyalität gegenüber dem Staat und der Anforderung der Sachlichkeit und Wahrhaftigkeit der amtlichen Mitteilung.

In beiden Systemen kann die Vernachlässigung von Pflichten (z. B. die Nichtüberprüfung der Einstufung des KI-Systems als „hochriskant“ oder die Freigabe von KI-generierten Mitteilungen ohne menschliche Aufsicht) zu Vorwürfen der mangelnden Sorgfalt und zu rechtlichen Konsequenzen führen. Ebenso sind Beamte in beiden Ländern individuellen disziplinarischen und finanziellen Konsequenzen ausgesetzt, wobei jedoch zu beachten ist, dass der institutionelle Schutz in Deutschland umfassender ist.

Adam JASKULSKI

KAPITEL V. ETHISCHE UND DATENSCHUTZRELEVANTE ASPEKTE DER NUTZUNG KÜNSTLICHER INTELLIGENZ IM KRISENMANAGEMENT

5.1. Einführung

Der vorliegende Teil des Berichts konzentriert sich auf den Einsatz von Instrumenten (Systemen) der künstlichen Intelligenz (KI) im Krisenmanagement zwischen Polen und der Bundesrepublik Deutschland, einerseits aus der Perspektive der EU-Vorschriften zum Schutz personenbezogener Daten (DSGVO) und andererseits aus der Perspektive der ethischen Nutzung künstlicher Intelligenz.

5.2. DSGVO und KI

Die Analyse des AI Act im Zusammenhang mit der DSGVO zeigt bestimmte Ähnlichkeiten zwischen diesen Rechtsakten auf. Das Regulierungsmodell beider Verordnungen unterscheidet sich nämlich erheblich von den Regulierungsmodellen nationaler Gesetze, da es sich auf die Ziele und Ergebnisse konzentriert, die von den zur Anwendung beider Rechtsakte verpflichteten Stellen erreicht werden sollen, und nicht unbedingt immer genau angibt, wie diese Ziele oder Ergebnisse in der Praxis erreicht werden sollen. Gleichzeitig gilt jedoch die Unfähigkeit, die Umsetzung geeigneter Maßnahmen nachzuweisen, die die Erfüllung der Verpflichtungen aus beiden Rechtsakten ermöglichen würden, als Verstoß gegen die Bestimmungen beider Rechtsakte seitens des Verpflichteten. Der gewählte Ansatz verpflichtet die Verpflichteten, nachzuweisen und zu belegen, dass ihre Maßnahmen im Einklang mit dem geltenden Recht standen.

Ein weiteres gemeinsames Merkmal dieser Rechtsakte, insbesondere im Falle des AI Act, ist der hohe Anteil an Fachterminologie, was die Arbeit mit diesen Rechtsvorschriften für Personen ohne entsprechende Fachkenntnisse erschwert. In der Praxis der Krisenmanagementbehörden wird dies erfordern, dass großer Wert darauf gelegt wird, die Mitarbeiter insbesondere mit dem AI Act vertraut zu machen, wenn es um die Einführung und Anwendung von KI-basierten Tools geht, aber auch unter Berücksichtigung der Vorschriften zum Schutz personenbezogener Daten.

Drittens ergibt sich die Besonderheit dieser Rechtsakte auch aus der großen Bedeutung, die den Leitlinien der Aufsichtsbehörden beigemessen wird, die durch beide Rechtsakte sowohl auf Ebene der Europäischen Union als auch in den einzelnen Mitgliedstaaten eingerichtet wurden. Auch wenn die Leitlinien nicht rechtsverbindlich sind, werden sie für die Anwendung beider Rechtsakte von entscheidender Bedeutung sein, weshalb die Beamten ihr Wissen auf der Grundlage der herausgegebenen Leitlinien aktualisieren müssen. Im Falle der DSGVO gibt es aufgrund ihrer seit mehreren Jahren bestehenden Anwendung im Rechtsverkehr bereits eine beträchtliche Anzahl von

Leitlinien. Die Leitlinien zur Anwendung des KI-Gesetzes sowie die Leitlinien zum Verhältnis beider Verordnungen werden hingegen erst noch erstellt.

Die Anwendung der DSGVO-Vorschriften auf den Einsatz von KI-Systemen erfordert die Einhaltung aller Grundsätze, auf denen die Datenschutzverordnung basiert. Dies sind die folgenden Grundsätze: Rechtmäßigkeit, Fairness und Transparenz; Zweckbindung der Verarbeitung personenbezogener Daten; Datenminimierung; Richtigkeit der personenbezogenen Daten (Aktualität/Wahrhaftigkeit); Speicherbegrenzung (Datenaufbewahrung); Integrität und Vertraulichkeit; Rechenschaftspflicht (Fähigkeit, die ordnungsgemäße Funktion des Datenschutzsystems nachzuweisen). Darüber hinaus sind die Rechte der betroffenen Personen zu nennen, d. h.: Recht auf Information, Auskunft, Berichtigung, Löschung („Recht auf Vergessenwerden"), Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch.

Aufgrund des begrenzten Umfangs dieser Veröffentlichung werden nur einige dieser Grundsätze im Zusammenhang mit KI-Systemen behandelt, da sie für einen angemessenen Schutz personenbezogener Daten von grundlegender Bedeutung sind. Zu den übrigen Grundsätzen gibt es eine sehr umfangreiche Literatur sowohl zur DSGVO selbst als auch zur DSGVO im Zusammenhang mit KI.

Zunächst einmal ist zu betonen, dass die DSGVO den Schwerpunkt auf den Schutz personenbezogener Daten und Transparenz legt. Leider sind diese Grundsätze im Falle der KI oft schwer miteinander zu vereinbaren. Das wohl bekannteste Problem ist die Herausforderung der „Black Box" von KI-Algorithmen, was bedeutet, dass es bei vielen fortschrittlichen Algorithmen, insbesondere solchen, die auf Deep Learning basieren, schwierig ist, zu verstehen und zu erklären, warum der Algorithmus eine bestimmte Entscheidung getroffen hat. Das System präsentiert bestimmte Ergebnisse seiner Tätigkeit, aber es fehlen Informationen darüber, welche Faktoren zu diesen Ergebnissen geführt haben. Dies verletzt das Recht einer Person auf Information, da sie keine Möglichkeit hat, herauszufinden, warum der Algorithmus eine bestimmte Entscheidung getroffen hat, die sie betrifft. In diesem Fall ist es notwendig, die Technik der erklärbaren KI (engl. Explainable AI, XAI) anzuwenden, um zu verstehen, wie KI-Algorithmen Entscheidungen treffen. Es gibt Tools zur Visualisierung und Interpretation von Algorithmusentscheidungen, sodass es möglich ist, „Erklärungen" für Benutzer zu erstellen und KI-Entscheidungsprozesse zu dokumentieren. Daher ist es wichtig, beim Erwerb bestimmter KI-basierter Tools von deren Anbietern Unterlagen anzufordern, die eine rechtmäßige Nutzung durch den Anwender der KI-Systeme gewährleisten. Die Übersetzung der Dokumentation zu KI-Algorithmen ist, wenn solche Systeme im grenzüberschreitenden Krisenmanagement eingesetzt werden sollen, unerlässlich, um sicherzustellen, dass alle verstehen, wie diese Algorithmen funktionieren und welche personenbezogenen Daten sie verarbeiten. Die Erläuterung kultureller Unterschiede im Umgang mit dem Datenschutz ist ebenfalls wichtig, um Missverständnisse und Konflikte zwischen den Verantwortlichen auf beiden Seiten der deutsch-polnischen Grenze zu vermeiden.

Zweitens ist es bei der Umsetzung von KI-Projekten, die mit einem hohen Risiko für die Verletzung der Privatsphäre verbunden sein können, erforderlich, in Zusammenarbeit mit dem Datenschutzbeauftragten eine Datenschutz-Folgenabschätzung (Data Protection Impact Assessment – DPIA) durchzuführen. Es ist erforderlich, die Risiken für die Privatsphäre natürlicher Personen zu ermitteln und zu bewerten, Maßnahmen zur Minimierung des Risikos einer Verletzung der Privatsphäre zu ergreifen und gegebenenfalls die zuständige Datenschutzaufsichtsbehörde zu konsultieren. Bei der Einführung von KI-basierten Lösungen für das Krisenmanagement ist es daher erforderlich, die entsprechenden

Dokumente zum Schutz personenbezogener Daten durch die zuständigen Behörden zu aktualisieren und die neuen Leitlinien der zuständigen Behörden laufend zu verfolgen.

Drittens, und das ist entscheidend, muss der Schutz personenbezogener Daten bereits bei der Entwicklung von KI-Systemen berücksichtigt werden. Daher sollten Systeme so konzipiert werden, dass sie die Datenerfassung standardmäßig minimieren, und es sollten Mechanismen zur Kontrolle des Datenzugriffs gemäß dem Grundsatz „Privacy by Design“ eingeführt werden.[57]. In der Praxis der öffentlichen Verwaltung werden die Mitarbeiter zwar selten an der Entwicklung solcher Tools beteiligt sein, aber wenn diese Tools dann zum Einsatz kommen, müssen sie kontrollieren, ob der Schutz personenbezogener Daten bei der Konzeption und Entwicklung eines bestimmten KI-basierten Systems tatsächlich berücksichtigt wurde. Daher ist es notwendig, interne und externe Audits durchzuführen, die Einhaltung der DSGVO zu überwachen und Korrekturen und Verbesserungen vorzunehmen.

Viertens muss die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Grundsatz der Rechtmäßigkeit jeweils auf einer konkreten (individualisierten) Rechtsgrundlage für die Verarbeitung erfolgen. Es kann schwierig sein, eine gültige Einwilligung zur Verarbeitung von Daten durch KI zu erhalten, insbesondere wenn die KI die Daten auf eine Weise verarbeitet, die für die betroffene Person nicht nachvollziehbar ist. Die Einwilligung muss freiwillig, konkret, bewusst und eindeutig sein[58]. Die Verwendung von „Dark Patterns” zur Manipulation der Einwilligung ist unzulässig.

Die zweite Rechtsgrundlage für die rechtmäßige Verarbeitung personenbezogener Daten, die in der öffentlichen Verwaltung angewendet wird, ist hingegen der Fall, dass „die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde”[59]. Über die Herausforderungen im grenzüberschreitenden Krisenmanagement im Zusammenhang mit der Anwendung dieses Grundsatzes im weiteren Verlauf des Berichts.

5.3. Herausforderungen für KI im grenzüberschreitenden Krisenmanagement zwischen Polen und der Bundesrepublik Deutschland unter Berücksichtigung der DSGVO-Vorschriften

Die erste zentrale Herausforderung sind die Unterschiede in der Auslegung und Umsetzung der DSGVO zwischen Polen und Deutschland. Obwohl beide Länder Mitglieder der Europäischen Union sind und der DSGVO unterliegen, deren Inhalt in der gesamten EU identisch ist, kann es in der Praxis zu subtilen Unterschieden im Umgang mit dem Schutz personenbezogener Daten kommen.

Diese Unterschiede resultieren aus unterschiedlichen rechtlichen, kulturellen und organisatorischen Traditionen, insbesondere aus der Tätigkeit der Aufsichtsbehörde in jedem dieser Mitgliedstaaten. Die Unterschiede können beispielsweise die Verfahren zur Einholung der Einwilligung zur Verarbeitung personenbezogener Daten, den Ansatz zum Grundsatz der Datenminimierung oder die Auslegung des „wichtigen öffentlichen Interesses” als Rechtsgrundlage für die Verarbeitung personenbezogener Daten

57 Der Kern dieses Grundsatzes besteht darin, den Schutz personenbezogener Daten zum frühestmöglichen Zeitpunkt, d. h. bereits in der Entwurfsphase des Systems, zu implementieren. Infolgedessen ist das System von Anfang an darauf ausgerichtet, ein angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten.

58 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) Art. 4 Nr. 11, ABl. L 119 vom 4.5.2016, (Zugang: 06.10.2025).

59 Ibidem, Art. 6 Abs. 1 Buchst.) e.

betreffen. Infolgedessen können der Datenaustausch und die Zusammenarbeit zwischen öffentlichen Einrichtungen beider Länder in Krisensituationen aufgrund mangelnder Übereinstimmung hinsichtlich der Anwendung der DSGVO-Vorschriften erschwert sein.

Im Falle der Bundesrepublik Deutschland wird aufgrund der rechtlichen Traditionen und historischen Gegebenheiten ein wesentlich stärkerer Schwerpunkt auf den Schutz der Rechte des Einzelnen gelegt, was sich auch auf den Bereich des Datenschutzrechts auswirkt. Dies führt zu einem restriktiveren Ansatz in Bezug auf die oben genannten Fragen im Bereich des Datenschutzes, was sich in der Tätigkeit der zuständigen Datenschutzbehörden auf dem Gebiet der Bundesrepublik Deutschland widerspiegelt. An dieser Stelle sei darauf hingewiesen, dass die strengere Kontrolle der Einhaltung der DSGVO auf dem Gebiet der Bundesrepublik Deutschland auch auf eine umfangreichere Verwaltung zurückzuführen ist, die sich diesem Thema widmet. Neben dem Beauftragten auf Bundesebene sind auch die Behörden auf Ebene der einzelnen Bundesländer für die Überwachung der Einhaltung der Datenschutzbestimmungen zuständig. Besonderes Augenmerk wird in Deutschland auf die Aktualisierung von Richtlinien, Verfahren und Instrumenten zum Schutz personenbezogener Daten im Zusammenhang mit der technologischen Entwicklung gelegt. Daher ist mit einer erheblichen Aktivität der genannten Behörden im Zusammenhang mit den Veränderungen und vor allem den Herausforderungen zu rechnen, die sich aus der Einführung von KI-basierten Lösungen und deren Umsetzung im Bereich des Datenschutzes ergeben.

Eine weitere große Herausforderung sind sprachliche und kulturelle Barrieren. Sprache ist nicht nur ein Kommunikationsmittel, sondern auch ein Träger von Kultur und Werten. Kulturelle Unterschiede können beeinflussen, wie wir Privatsphäre wahrnehmen, wie wir die DSGVO-Vorschriften verstehen und wie wir Zusammenarbeit angehen. Sprachliche und kulturelle Barrieren können die Kommunikation und Zusammenarbeit zwischen öffentlichen Einrichtungen beider Länder erschweren, was zu Fehlern und Verzögerungen bei der Entscheidungsfindung führen kann. Dies gilt auch für das Verständnis von KI-Algorithmen, die in einer Sprache und Kultur entwickelt und in einer anderen verwendet werden können.

Die Übermittlung personenbezogener Daten zwischen Polen und Deutschland muss sicher und in Übereinstimmung mit der DSGVO erfolgen. Das bedeutet, dass geeignete technische und organisatorische Maßnahmen getroffen werden müssen, um die Daten vor unbefugtem Zugriff, Verlust oder Zerstörung zu schützen. Leider kann dies in der Praxis schwierig sein, insbesondere in Krisensituationen, in denen Zeit eine wichtige Rolle spielt und ein schnelles und effizientes Handeln der Dienste erforderlich ist.

Die Praxis des Datenschutzes in Polen zeigt, dass Eingriffe der Aufsichtsbehörde in den allermeisten Fällen aufgrund von Vorfällen im Zusammenhang mit Verletzungen des Schutzes personenbezogener Daten erfolgen. In Deutschland wird viel mehr Wert auf die Gewährleistung der Konformität personenbezogener Daten in Echtzeit gelegt, also durch Audits, Schulungen und Aktualisierungen der erforderlichen Dokumente.

5.4. Lösungen und bewährte Verfahren im grenzüberschreitenden Krisenmanagement mit KI

Der erste wichtige Schritt ist die Ausarbeitung gemeinsamer Datenschutzstandards für das grenzüberschreitende Krisenmanagement. Diese Standards sollten die Rechte der Bürger bei der Verarbeitung personenbezogener Daten festlegen, welche Daten von Behörden verarbeitet werden

dürfen, zu welchem Zweck, wie lange sie gespeichert werden dürfen und welche Sicherheitsmaßnahmen von den einzelnen Behörden in beiden Mitgliedstaaten angewendet werden.

Rechtlich gesehen wären dies keine rechtsverbindlichen Standards, da natürlich keine Behörde, weder in Polen noch in Deutschland, befugt ist, solche Standards (Leitlinien) für andere Behörden festzulegen. Dennoch wäre es von entscheidender Bedeutung, Diskussionen zu führen und die Unterschiede in der Anwendung der betreffenden Bestimmungen der DSGVO zu klären, um Probleme bei der Zusammenarbeit auf operativer Ebene zu beseitigen. Ein solcher Ansatz würde eine effektive Zusammenarbeit in Krisensituationen ermöglichen und die zuständigen Behörden nicht daran hindern, personenbezogene Daten zwischen Polen und Deutschland zu übermitteln.

Eine empfohlene Lösung wäre auch, die zu ergreifenden Maßnahmen mit den zuständigen Datenschutzbehörden in jedem dieser Länder abzustimmen. Dies sind notwendige Maßnahmen, die unverzüglich ergriffen werden sollten, um gemeinsame Verfahren für Krisensituationen vorzubereiten und nicht erst bei deren Eintreten die Rechtsgrundlagen und Verfahren für die Übermittlung personenbezogener Daten zu analysieren. Wie bereits erwähnt, wird eher auf deutscher Seite ein stärkerer Druck zum Schutz personenbezogener Daten ausgeübt werden, was auch die für das Krisenmanagement zuständigen polnischen Behörden zu entsprechenden Anpassungen zwingen wird, die manchmal sogar als über das übliche Maß hinausgehend angesehen werden, wenn personenbezogene Daten grenzüberschreitend von Deutschland nach Polen übermittelt werden sollen.

Es ist zu betonen, dass intensive Arbeit an der Ausarbeitung von Kooperationsstandards notwendig ist, da uneinheitliche Datenschutzstandards zu Verstößen gegen die DSGVO, mangelndem Vertrauen zwischen den Institutionen und Verzögerungen bei der Reaktion auf Krisen führen können.

Angesichts der im Bericht erörterten potenziellen Anwendung von KI-Instrumenten, unter anderem in der Kommunikation und im Bereich der Bekämpfung von Desinformation, ist darauf hinzuweisen, dass eine der Möglichkeiten für den Einsatz solcher Instrumente darin besteht, Informationen/Meldungen an Mobiltelefone von Personen zu senden, die sich im Krisengebiet aufhalten, oder an Telefonnummern, die in bestimmten Systemen registriert sind. In diesem Fall betrifft die Verarbeitung personenbezogener Daten die potenzielle Verarbeitung der Telefonnummern der Personen, die von solchen Benachrichtigungen betroffen sind.

An dieser Stelle muss jedoch zwischen zwei Varianten der oben genannten Situation unterschieden werden. Wenn nämlich bei der standardmäßigen Übermittlung von Alarmmeldungen durch die zuständigen Krisenmanagementzentren, sei es in Polen oder in Deutschland, die Übermittlung der Meldung darin besteht, dass die Mobilfunkbetreiber verpflichtet werden, bestimmte Warnungen an die Mobilfunknutzer in einem bestimmten Gebiet zu senden, dann erfolgt in diesem Fall keine Verarbeitung personenbezogener Daten durch diese öffentlichen Stellen (Krisenmanagement), da sie keinen Zugriff auf die Nummern haben, an die diese Benachrichtigungen gesendet wurden. Bei verschiedenen Arten von Anwendungen, Websites oder Kommunikationskanälen, die für die Kommunikation mit den Einwohnern bestimmt sind und eine vorherige Registrierung durch den Nutzer erfordern, beispielsweise durch Angabe einer Telefonnummer, handelt es sich hingegen um eine Verarbeitung personenbezogener Daten.

Was die Instrumente zur Bekämpfung von Desinformation und Fake News angeht, so wird es zum gegenwärtigen Zeitpunkt aufgrund zahlreicher Unzulänglichkeiten nicht möglich sein, die gängigsten

KI-Systeme einzusetzen. Angesichts ihres Entwicklungsmodells scheint dies auch in absehbarer Zukunft nicht möglich zu sein. Dies ist unter anderem auf folgende Probleme zurückzuführen: Die verfügbaren Modelle arbeiten nicht mit vollständig aktuellen Daten, es kommt zu Halluzinationen, Diskriminierung und auch zur absichtlichen „Fütterung" der gängigsten Modelle mit gefälschten Daten, um die erhaltenen Ergebnisse zu manipulieren.

Daher ist es notwendig, KI-Systeme zu entwickeln, die speziell auf die Bekämpfung von Desinformation und Fake News ausgerichtet sind und sich derzeit in der Entwicklungsphase befinden. Solche Systeme ermöglichen die Überwachung von sozialen Medien und Websites sowie die Identifizierung von Desinformationsmaterialien und Fake News. Daher wird es notwendig sein, Zugang zu kommerziellen Tools zu erhalten, die speziell auf die Lösung dieser Art von Problemen und Herausforderungen ausgerichtet sind. Andernfalls müssen die öffentlichen Verwaltungen beider Länder Anstrengungen unternehmen, um solche KI-basierten Systeme zu entwickeln, was höchstwahrscheinlich mit der Durchführung von öffentlichen Ausschreibungen verbunden sein wird. In solchen Situationen wird es von entscheidender Bedeutung sein, die Anforderungen an die gewünschten Systeme angemessen zu beschreiben.

Darüber hinaus ist zu betonen, dass der Einsatz von KI-Systemen zur Überprüfung der Richtigkeit von Informationen in den meisten Fällen letztendlich die Beteiligung des Menschen in der letzten Phase der Identifizierung solcher Materialien erfordern wird, um sicherzustellen, dass die Entscheidungen mit dem tatsächlichen Sachverhalt übereinstimmen.

Es ist davon auszugehen, dass solche Tools bei der Analyse des Internets, einschließlich sozialer Medien, eine erhebliche Menge an personenbezogenen Daten verarbeiten würden. Daher wird es notwendig sein, in Absprache mit den Aufsichtsbehörden und den Anbietern von KI-Systemen entsprechende Anpassungen in den Richtlinien zur Verarbeitung personenbezogener Daten vorzunehmen.

Was dabei zu beachten ist, ist die bestehende Überregulierung, die sich aus der DSGVO im Bereich des Schutzes personenbezogener Daten ergibt. Mit der Einführung der Datenschutz-Grundverordnung im Jahr 2016 zielte der EU-Gesetzgeber in erster Linie auf die Regulierung des Marktes der gewinnorientierten Unternehmen ab, insbesondere derjenigen, die mit personenbezogenen Daten Geld verdienen. Gleichzeitig wurden beispielsweise auch öffentliche Verwaltungsbehörden mit solchen Verpflichtungen übermäßig belastet. Daher wäre es wichtig, dass der EU-Gesetzgeber auf legislativer Ebene reagiert, um die Arbeit der öffentlichen Verwaltung insbesondere in Krisensituationen im Bereich der Verarbeitung personenbezogener Daten zu erleichtern. In diesem Fall würde die Nutzung von KI durch die öffentliche Verwaltung aus Sicht der DSGVO vereinfacht werden.

5.5. Ethische Fragen im Zusammenhang mit der Nutzung künstlicher Intelligenz

Die Frage der ethischen künstlichen Intelligenz (KI) ist aus Sicht der Gesetzgebung der Europäischen Union von zentraler Bedeutung und bildet einen der Grundpfeiler des KI-Gesetzes, d. h. der „Verordnung des Europäischen Parlaments und des Rates (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und

(EU) 2020/1828 (Künstliche-Intelligenz-Verordnung)“[60]. Bei der Ausarbeitung dieses Rechtsakts hat die Europäische Union erkannt, dass es von entscheidender Bedeutung ist, ein Gleichgewicht zwischen den Interessen der Entwickler von Systemen der künstlichen Intelligenz und denen der Gesellschaft herzustellen.

Die grundlegende ethische Prämisse des AI Act ist die Erkenntnis, dass künstliche Intelligenz im Dienste der Gesellschaft, zum Wohle des Einzelnen und unter menschlicher Kontrolle entwickelt werden muss. Künstliche Intelligenz soll dem Menschen dienen und darf unter keinen Umständen nicht nur rechtswidrig, sondern auch unethisch eingesetzt werden. Es ist sogar anzunehmen, dass bestimmte ethische Grundsätze den Status von Rechtsnormen erlangt haben. Da es sich bei der genannten Verordnung um eine EU-weite Verordnung handelt, gilt sie gleichermaßen für das Krisenmanagement in Polen wie auch in der Bundesrepublik Deutschland.

Die oben genannten ethischen Grundsätze sind für das Verständnis der ethischen Dimension der KI von entscheidender Bedeutung. Aufgrund des begrenzten Umfangs dieser Studie wurden sie nur in einem grundlegenden Umfang behandelt, der ein Verständnis der Haltung der EU zur Bedeutung der Ethik bei der Regulierung der KI ermöglicht. Es muss betont werden, dass die so skizzierten Grundsätze in allen Phasen der Arbeit an und mit künstlicher Intelligenz umgesetzt werden müssen. Diese Grundsätze müssen bereits in der Phase der Konzeption des KI-Systems, dann bei dessen Aufbau und Implementierung sowie in der Nutzungsphase umgesetzt werden. Wie bereits erwähnt, gilt dies auch für die gesetzliche Verpflichtung zum Schutz personenbezogener Daten.

Da das Krisenmanagement in Polen und Deutschland in die Zuständigkeit der öffentlichen Verwaltung auf verschiedenen Ebenen dieser beiden Staaten fällt, muss es naturgemäß ausschließlich auf der Grundlage des Rechts und innerhalb seiner Grenzen erfolgen. Beamte der öffentlichen Verwaltung sind darüber hinaus häufig an verschiedene Ethikkodizes gebunden, weshalb es für diese Personen besonders wichtig ist, die ethischen Grundlagen des Einsatzes von KI-Systemen in ihrer Arbeit zum Wohle der Bürger zu verstehen.

Es ist zu betonen, dass im Falle von Mitarbeitern von Krisenmanagementdiensten ethische Grundsätze vor allem bei der Nutzung bereits entwickelter KI-Systeme Anwendung finden, während sie bei der Konzeption, Entwicklung und Implementierung eher in begrenztem Umfang zum Tragen kommen. Hochriskante KI-Systeme unterliegen einer gesetzlichen Audit- und Modifikationspflicht, um ihre rechtmäßige Funktionsweise sicherzustellen. Selbst wenn also in den allermeisten Fällen die für das Krisenmanagement zuständigen Beamten die Nutzer dieser Systeme sind, sind sie dennoch zu deren ethischer Nutzung verpflichtet, und etwaige festgestellte unethische Handlungen von KI-Systemen sollten den zuständigen Personen gemeldet und aus diesen Systemen entfernt werden.

Ein weiterer wichtiger Aspekt ist die angemessene Schulung der für das Krisenmanagement zuständigen Beamten in den Bereichen DSGVO, KI-Ethik und Datensicherheit. Die Mitarbeiter müssen verstehen, welche Pflichten sie haben und wie sie sich gesetzes- und ethikkonform verhalten müssen. Durch Schulungen für Mitarbeiter von Krisenmanagementzentren zum Thema Verarbeitung

60 VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) ABl. L, 2024/1689, 12.7.2024, (Zugang am: 06.10.2025).

personenbezogener Daten in Notfällen können Fehler und Rechtsverstöße vermieden werden. Diese Schulungen und Workshops sollten regelmäßig stattfinden, da beispielsweise die Richtlinien zur DSGVO und zum KI-Gesetz aktualisiert und Ethikkodizes für die Anwendung dieser Rechtsakte eingeführt werden. Darüber hinaus wird insbesondere der Bereich der KI technologisch sehr stark weiterentwickelt, und es ist davon auszugehen, dass sich dieser Prozess in den kommenden Jahren sogar noch intensivieren wird. Daher ist es notwendig, auch in diesem Bereich das Wissen zu ergänzen.

Trotz der bestehenden rechtlichen, politischen, organisatorischen und finanziellen Einschränkungen wäre es im Bereich des grenzüberschreitenden Krisenmanagements wünschenswert, eine Harmonisierung der im grenzüberschreitenden Krisenmanagement eingesetzten KI-Systeme anzustreben, und noch wünschenswerter wäre die Schaffung gemeinsamer KI-Tools für das deutsch-polnische Grenzgebiet. Eine solche Entscheidung ermöglicht es, zwei grundlegende Risiken zu beseitigen, die bei der Verwendung solcher Tools bestehen. Erstens: Das Training der Daten nur auf der Grundlage eines Datensatzes aus einem einzigen Land, was es unmöglich macht, eine grenzüberschreitende Perspektive zu erfassen, und dazu führen kann, dass KI-Systeme aufgrund des Trainings mit unvollständigen Daten diskriminierende Entscheidungen treffen. Zweitens ermöglichen solche Lösungen die Beseitigung von Sprachproblemen, wenn ein grenzüberschreitendes System unter Verwendung von Daten oder Testern aus beiden Ländern gleichzeitig entwickelt würde. Dann könnten alle sprachlichen Nuancen, aber auch ähnliche organisatorische Probleme oder rechtliche Beschränkungen berücksichtigt werden.

Entscheidend für die Nutzung von KI im Einklang mit den ethischen Grundsätzen unserer Gesellschaften ist auch das Verständnis, dass selbst wenn KI bestimmte Entscheidungen schneller und treffender trifft, es niemals dazu kommen darf, dass wir, auch nur in bestimmten Bereichen, die gesamte Verantwortung für bestimmte Entscheidungen auf die künstliche Intelligenz übertragen. Technologie ist unzuverlässig, aber vor allem dürfen wir als Gesellschaft und als einzelne Individuen unsere Fähigkeit zum kritischen Denken und vor allem unsere Kompetenz zur Lösung bestimmter Probleme nicht verlieren, da sonst dem Menschen, dem die KI untergeordnet sein soll, die Fähigkeit fehlt, die Richtigkeit der von der KI getroffenen Entscheidungen zu beurteilen.

5.6. Die Bedeutung der sozialen Bildung im Bereich der ethischen KI

Der Schlüssel zu einer verantwortungsvollen und effektiven Umsetzung von KI, insbesondere im Bereich des Krisenmanagements, liegt darin, sicherzustellen, dass die Öffentlichkeit, Entscheidungsträger und Technologieentwickler über fundierte Kenntnisse der Möglichkeiten, Grenzen und vor allem der ethischen Implikationen dieser Technologie verfügen. Ohne ein breites Bewusstsein kann KI als „schwarze Magie" (das Problem der „Black Box") wahrgenommen werden, was zu Angst, Misstrauen oder bei manchen Menschen sogar zum Gegenteil führt, nämlich zur unkritischen Akzeptanz potenziell schädlicher Lösungen. Diese negativen Folgen sind im Bereich des Krisenmanagements besonders gefährlich, da es sich dabei jeweils um Maßnahmen handelt, die unter enormem Zeitdruck, unter Bedingungen der Unsicherheit und Informationslücken und vor allem in einer Situation getroffen werden, in der Leben und Gesundheit von Menschen gefährdet sind und die Gefahr erheblicher Sachschäden besteht.

Die Bildung sollte nicht nur die technischen Aspekte der KI umfassen, sondern auch ihre Auswirkungen auf die Gesellschaft, die Wirtschaft, die Menschenrechte und ethische Werte. Besonderes Augenmerk

sollte auf die Entwicklung kritischer Denkfähigkeiten gelegt werden, die es den Bürgern ermöglichen, die Glaubwürdigkeit von Informationen zu beurteilen und fundierte Entscheidungen über die Nutzung der KI zu treffen.

Auf Seiten der Krisenmanagementbehörden wird es erforderlich sein, für alle zugängliche Bildungsmaterialien in Form von Filmen, Infografiken, Artikeln oder Online-Kursen zu erstellen. Diese Bildungsmaterialien sollten leicht zugänglich, verständlich und an verschiedene Altersgruppen und Wissensstände angepasst sein. Bei der Einführung solcher Instrumente für den Einsatz in Krisensituationen sollte eine Testanwendung unter Beteiligung einer beträchtlichen Anzahl von Einwohnern durchgeführt werden, um die Funktionen solcher Instrumente, gegebenenfalls ihre Grenzen, aber auch die Möglichkeit, sich an einen Menschen zu wenden, um eine vom KI-System getroffene Entscheidung zu erklären oder zu bestätigen, aufzuzeigen.

Es ist notwendig, bei den Bürgern Vertrauen in solche Instrumente aufzubauen, damit sie in Krisensituationen bereit sind, ihnen zu vertrauen. Das mangelnde Vertrauen der Einwohner in KI-Systeme, die im Krisenmanagement eingesetzt werden, insbesondere im Bereich der Kommunikation mit den Einwohnern, der Hilfeleistung oder sogar der psychologischen Unterstützung, führt dazu, dass diese Systeme praktisch nutzlos sind und in Extremsituationen sogar noch mehr Chaos verursachen können. Daher müssen solche Instrumente sehr sorgfältig und unter breiter Beteiligung der Bevölkerung in der Test- und Einführungsphase eingesetzt werden, damit sie in realen Krisensituationen ihre Funktionen ordnungsgemäß erfüllen können.

Es ist systemisch notwendig, die öffentliche Debatte über KI und Ethik zu fördern, indem Massenmedien, Nichtregierungsorganisationen und öffentliche Einrichtungen einbezogen werden, die sich aktiv an der Diskussion über KI und ihre Auswirkungen auf die Gesellschaft beteiligen sollten. Dies liegt in erster Linie in der Verantwortung der Regierungsbehörden, da es sich um eine Verpflichtung aus dem KI-Gesetz handelt.

Die Information über den Einsatz von KI bei Entscheidungen oder Maßnahmen ist aus Sicht der Empfänger von entscheidender Bedeutung. Aus rein menschlicher und damit auch aus ethischer Sicht wird diese Information jedoch für viele Menschen dazu führen, dass sie den Kontakt mit solchen Tools meiden, Unruhe empfinden oder aufgrund der fehlenden Beteiligung des menschlichen Faktors an der Entscheidungsfindung von der Unrichtigkeit der getroffenen Entscheidung überzeugt sind. Diese Art der Entmenschlichung wird für viele Menschen sehr schwer zu akzeptieren sein. Beispielsweise wäre es nicht ratsam, die Entscheidung über die Nichtzulassung eines Kindes zur Schule durch KI treffen zu lassen. In einer solchen Situation würden die meisten Menschen Verwirrung und Unbehagen empfinden und diese Tatsache anzweifeln.

Ebenso wichtig ist, dass in Krisensituationen aus Sicht des Krisenmanagements die Information der Öffentlichkeit darüber, dass bestimmte Entscheidungen in Zusammenarbeit mit KI oder sogar durch KI getroffen wurden, zu einer erheblichen Verringerung der Akzeptanz solcher Entscheidungen oder Maßnahmen führen könnte.

Es handelt sich also um ein rechtliches und ethisches Dilemma, da wir uns einerseits der Richtigkeit von Entscheidungen bewusst sind, die unter Mitwirkung von KI getroffen werden, sofern natürlich alle Bedingungen für die Korrektheit ihrer Entscheidungsfindung erfüllt sind. Andererseits sind wir uns der Schwierigkeit bewusst, dass solche Entscheidungen von einzelnen Mitgliedern der Gesellschaft

akzeptiert werden. Es stellt sich also die ethische Frage, ob man die Gesellschaft oder bestimmte Personen nicht über den Einsatz von KI zur Entscheidungsfindung informieren sollte, um insbesondere in Krisensituationen, in denen das Vertrauen der Menschen in die getroffenen und manchmal ihnen auferlegten Entscheidungen von entscheidender Bedeutung ist (im Rahmen der Verwaltungshoheit öffentlicher Stellen). Wie bereits erwähnt, schreibt das Gesetz jedoch vor, dass die Menschen über solche Situationen informiert werden müssen, sodass die Nichtkennzeichnung von Material, das mit künstlicher Intelligenz erstellt wurde, einen Verstoß gegen das Gesetz darstellen würde.

Wie oben erwähnt, können KI-Systeme zur Identifizierung von Desinformation, Fake News und Deep Fakes eingesetzt werden (und werden dies teilweise bereits). Es besteht also die Möglichkeit, sie auch im Bereich des Krisenmanagements einzusetzen. Wie bereits erwähnt, ist jedoch die Voraussetzung für ihren wirksamen Einsatz zur Bekämpfung dieser Phänomene einerseits die Schaffung von Vertrauen der Öffentlichkeit in KI-Systeme und andererseits das Vertrauen der Öffentlichkeit als Ganzes in die öffentliche Verwaltung (politische Macht, Regierung, Behörden auf verschiedenen Ebenen) im Bereich der Bekämpfung von Desinformation und Fake News. Selbst die besten KI-basierten Systeme zur Bekämpfung von Desinformation, Fake News und Deep Fakes werden sich als völlig nutzlos erweisen, wenn ein Teil der Bevölkerung kein Vertrauen in solche Instrumente und die offiziellen Verlautbarungen der politischen Entscheidungsträger hat.

5.7. Kommentar zu den Forschungsergebnissen

Die durchgeführten Umfragen zeigen, dass die Befragten nicht vollständig über die Möglichkeiten und Einsatzbereiche von KI informiert sind, nicht nur im privaten, sondern vor allem im beruflichen Leben. Insbesondere die weit verbreitete Überzeugung, dass KI nicht in der Lage ist, bessere Entscheidungen zu treffen als Menschen, ist falsch. Das Wissen, über das wir derzeit über KI verfügen, zeigt, dass sie bei der Entscheidungsfindung grundsätzlich fehlerfreier ist als der Mensch. Im Rahmen der ethischen Fragen der Nutzung von KI ist es jedoch, wie bereits in diesem Teil des Berichts dargelegt, unerlässlich, einen starken Schwerpunkt auf die Aufklärung über KI sowohl bei Beamten der öffentlichen Verwaltung, einschließlich der für das Krisenmanagement zuständigen Personen, als auch in der gesamten Gesellschaft zu legen. Es bedarf fundierter, aktueller Kenntnisse über die Funktionsweise von KI, die Vorteile, aber auch die Mängel dieser Instrumente.

Die durchgeführten Untersuchungen zeigen, dass ein Teil der Befragten, um es ganz offen zu sagen, KI dämonisiert – 11 % der Befragten sind der Meinung, dass KI eine Gefahr für die gesamte Menschheit darstellt, und über 22 % stimmen dieser Aussage weder zu noch widersprechen sie ihr.

Auf dieser Grundlage sollten zwei Risiken definiert werden, die sich aus dieser Wahrnehmung von KI ergeben. Erstens die begrenzte Bereitschaft, KI-Tools zu nutzen und Entscheidungen darauf zu stützen, da die Studie gezeigt hat, dass die Personen, die diese Tools einsetzen sollen, ihnen teilweise misstrauen. Zweitens, was noch wichtiger ist: Da KI von einem Teil der für das Krisenmanagement verantwortlichen Personen auf die oben beschriebene Weise wahrgenommen wird, wird es sehr schwierig sein, die Durchschnittsbevölkerung davon zu überzeugen, den von KI generierten Entscheidungen zu folgen, was gerade in Krisensituationen von besonderer Bedeutung ist. Wie oben bereits erwähnt, ist Aufklärung notwendig, um diese Wahrnehmung von KI zu überwinden.

Die Ergebnisse der Studie zeigen auch, dass das Rechtswissen über die DSGVO, die bereits seit sieben Jahren in Kraft ist, insbesondere im Zusammenhang mit dem zuvor geltenden Recht zum Schutz

personenbezogener Daten, zu gering ist und dass auch das Rechtswissen über den AI Act unzureichend ist. Dies stellt eine grundlegende Gefahr für die rechtmäßige Nutzung künstlicher Intelligenz dar. Es ist von entscheidender Bedeutung, dass die politischen Entscheidungsträger darauf achten, dass die für das Krisenmanagement zuständigen Personen eine intensive juristische Ausbildung erhalten, um die Anzahl der Situationen zu minimieren, die zu Verstößen gegen das Gesetz oder die DSGVO führen könnten. Ein größeres Wissen unter den Beamten wird zu mehr Selbstvertrauen und damit zu einer intensiveren Nutzung von KI in ihrer Arbeit führen.

Es ist zu betonen, dass es die politischen Entscheidungsträger sind, die den regulatorischen Rahmen für die Tätigkeit der öffentlichen Verwaltung nicht nur in Polen und Deutschland, sondern in der gesamten Europäischen Union schaffen. Sie legen auch weitgehend die Richtung der politischen Tätigkeit der öffentlichen Verwaltung fest und sind für die Einführung von Innovationen in deren täglicher Arbeit verantwortlich. Die Umsetzung von KI-basierten Lösungen muss daher mit der politischen Akzeptanz dieser Maßnahmen einhergehen. Daher müssen in erster Linie die politischen Entscheidungsträger auf allen Ebenen der öffentlichen Verwaltung das Potenzial der KI-Nutzung und die damit verbundenen Risiken verstehen. Aufgrund der Ergebnisse der durchgeführten Untersuchungen kann davon ausgegangen werden, dass auch in dieser Gruppe erhebliche Unkenntnis und Skepsis gegenüber dem Einsatz von KI-basierten Instrumenten besteht. Ohne die Überwindung dieser Hindernisse durch Aufklärung wird es nicht möglich sein, KI tatsächlich in der öffentlichen Verwaltung, einschließlich des Krisenmanagements, einzuführen.

Schlussfolgerungen für die Zukunft

Der vorliegende Bericht konzentriert sich auf den Einsatz von KI-Systemen im grenzüberschreitenden Krisenmanagement im Bereich der Kommunikation und der Bekämpfung von Desinformation. Um den Herausforderungen der Zukunft gerecht zu werden, muss jedoch darauf hingewiesen werden, dass dies nicht die einzigen Anwendungsbereiche von KI im Krisenmanagement sind. Daher sollten diese Möglichkeiten bereits jetzt den für das Krisenmanagement Verantwortlichen signalisiert werden. Erstens kann KI in Krisensituationen zur Festlegung und Aktualisierung von Evakuierungswegen für die Bevölkerung eingesetzt werden, die grenzüberschreitend verlaufen können. Zweitens besteht die Möglichkeit, KI für die Steuerung von Migrationsbewegungen einzusetzen, beispielsweise in Situationen wie dem Beginn der russischen Invasion in der Ukraine im Februar 2022, die zu einem plötzlichen Massenzustrom von Kriegsflüchtlingen zunächst nach Polen und dann über die gemeinsame Grenze nach Deutschland führte.

Drittens können öffentliche Einrichtungen in Krisensituationen wie Naturkatastrophen, Pandemien oder Terroranschlägen KI einsetzen, um diese Daten zu analysieren, Risiken zu identifizieren, Entwicklungen vorherzusagen und die Ressourcenverteilung zu optimieren. Bei grenzüberschreitenden Gefahren ist es wichtig, KI-Systeme zu verwenden, die mit Daten aus beiden Ländern trainiert wurden, um das Risiko von Diskriminierung und Entscheidungen auf der Grundlage von Empfehlungen von KI-Systemen zu vermeiden, die nicht die Interessen beider Partner berücksichtigen. Viertens: Im Falle einer Pandemie wie COVID-19 können Standortdaten von Mobiltelefonen zur Verfolgung der Ausbreitung der Epidemie verwendet werden. In diesem Fall sollte besonderer Wert auf die angemessene Sicherung der Verarbeitung personenbezogener Daten gelegt werden.

Dariusz DYMEK

KAPITEL VI. ORGANISATORISCHE VERÄNDERUNGEN IM BEREICH DES KRISENMANAGEMENTS IN POLEN

Die gesellschaftlichen Erwartungen hinsichtlich einer Regelung des Bereichs Krisenmanagement zwangen die damaligen politischen Akteure zu einer Reihe von Zugeständnissen, die am 26. April 2007 zur Verabschiedung des Gesetzes über Krisenmanagement[61] führten. Dieses Gesetz schuf jedoch keine systemischen Lösungen, und sein Inhalt wurde und wird als eine Art politischer Kompromiss angesehen.

Das Gesetz führte Aufgaben und Pflichten im Zusammenhang mit dem Krisenmanagement für öffentliche Behörden ein, die mit denen der Krisenmanagementbehörden identisch sind. Die Definition des Krisenmanagements gemäß Artikel 2 des Gesetzes lautet: „Krisenmanagement ist eine Tätigkeit der öffentlichen Verwaltung, die Teil der nationalen Sicherheitsführung ist und darin besteht, Krisensituationen zu verhindern, sich darauf vorzubereiten, durch geplante Maßnahmen die Kontrolle über sie zu übernehmen, im Falle von Krisensituationen zu reagieren, ihre Folgen zu beseitigen und Ressourcen und kritische Infrastruktur wiederherzustellen".[62] Wie man sieht, wird weder das System noch eine andere Form der Abhängigkeit, Beziehung oder gegenseitigen Unterordnung der Krisenmanagementbehörden erwähnt. Die beispielhaften Zuständigkeiten der Krisenmanagementbehörde auf Gemeindeebene sind hingegen in Art. 19 des oben genannten Gesetzes charakterisiert. Zu den wichtigsten gehören die Leitung der Überwachung, Planung, Reaktion und Beseitigung der Folgen von Gefahren auf dem Gebiet der Gemeinde sowie die Verwaltung, Organisation und Durchführung von Schulungen, Übungen und Trainings im Bereich des Krisenmanagements. Diese und andere Aufgaben werden vom Gemeindevorsteher, Bürgermeister oder Stadtpräsident mit Hilfe der für Krisenmanagement zuständigen Organisationseinheit der Gemeinde- (Stadt-)Verwaltung wahrgenommen.

Gemäß dem Gesetz sollten auf jeder Ebene der öffentlichen Verwaltung (Gemeinde, Landkreis, Woiwodschaft und zentrale Ebene) Krisenmanagementteams als Beratungsgremien der Krisenmanagementbehörden, d. h. der Gemeindevorsteher, Landräte, Woiwoden oder des Ministerpräsidenten, eingerichtet werden. Darüber hinaus sollten auf zentraler, Woiwodschafts- und Kreisebene Stellen eingerichtet werden, die einen ungestörten 24-Stunden-Informationsfluss über die Sicherheitslage in dem jeweiligen Gebiet gewährleisten. So wurde auf zentraler Ebene das Regierungszentrum für Sicherheit, auf Woiwodschaftsebene das Woiwodschaftszentrum für Krisenmanagement (WCZK) und auf Kreisebene das Kreiszentrum für Krisenmanagement (PCZK) eingerichtet. Auf Gemeindeebene muss der Gemeindevorsteher, in unserem Fall der Bürgermeister, kein kommunales/städtisches Krisenmanagementzentrum (G/MCZK) einrichten, was für unser Projekt von

61 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Gesetz vom 26. April 2007 über das Krisenmanagement), BGBl. 2023 Nr. 122, (Zugang am: 06.10.2025).

62 Ibidem, S. 1.

entscheidender Bedeutung ist. Das Fehlen eines Bereitschaftsdienstes, der rund um die Uhr Überwachungsaufgaben wahrnimmt, Informationen im Zusammenhang mit der Sicherheit im weiteren Sinne sammelt und verarbeitet, führt dazu, dass diese Informationen nicht oder nur mit erheblicher Verzögerung bei der für das Krisenmanagement zuständigen Stelle, d. h. dem Bürgermeister, eingehen. Das Gesetz lässt leider das Fehlen eines G/MCZK zu, dessen Einrichtung ausschließlich im Ermessen der Gemeinde-/Stadtverwaltung liegt. Das Fehlen eines G/MCZK wird sehr oft durch einen Mitarbeiter ersetzt, der unter der sogenannten „Telefonnummer" Bereitschaftsdienst hat. In alltäglichen Situationen funktioniert dies gut, aber in Notfällen, insbesondere solchen mit sich entwickelnder Dynamik, leider nicht. Darüber hinaus ist anzumerken, dass eine der wichtigsten Aufgaben auf Gemeindeebene die Erkennung, Warnung und Alarmierung vor Gefahren ist. Zur Erfüllung dieser Aufgabe werden elektronische oder ältere elektrische Sirenen verwendet, die meist auf Gemeindeebene ausgelöst werden. Das Fehlen eines Bereitschaftsdienstes bedeutet auch, dass es nicht möglich ist, Sirenen auszulösen und die Bevölkerung vor einer drohenden Gefahr zu warnen oder zu alarmieren.[63].

Trotz des Fehlens eines G/MCZK sorgt der Gemeindevorsteher, Bürgermeister oder Stadtpräsident für die Umsetzung folgender Aufgaben im Gebiet der Gemeinde (Stadt):

1. Rund-um-die-Uhr-Alarmierung der Mitglieder des kommunalen Krisenstabs und in Krisensituationen Gewährleistung eines Rund-um-die-Uhr-Bereitschaftsdienstes, um den Informationsfluss sicherzustellen und die durchgeführten Maßnahmen zu dokumentieren,
2. Zusammenarbeit mit den Krisenstäben der öffentlichen Verwaltung,
3. Überwachung des Funktionierens des Erkennungs- und Alarmierungssystems sowie des Frühwarnsystems für die Bevölkerung,
4. Zusammenarbeit mit Stellen, die Umweltüberwachungsaufgaben wahrnehmen,
5. Zusammenarbeit mit Stellen, die Rettungs-, Such- und humanitäre Maßnahmen durchführen,
6. Wahrnehmung von Bereitschaftsdiensten zur Erhöhung der Verteidigungsbereitschaft des Staates.

Im Krisenmanagement gibt es neben den Behörden auch Krisenmanagementeinrichtungen, meist staatliche Einrichtungen, die Teil des Sicherheitsnetzes sind, dem wichtigsten Element jedes Krisenmanagementplans. Das Sicherheitsnetz ist eine Matrix, die den Standort und die Aufgaben der Krisenmanagementeinrichtungen im Hinblick auf potenzielle Gefahren festlegt und die federführende Einrichtung sowie die unterstützenden Einrichtungen benennt. Aus diesem Element des Plans ergibt sich die Zusammenarbeit vieler Einrichtungen im Falle einer konkreten Gefahr. Trotz fast zwei

63 Bei der Erstellung dieses Berichts kam es am 10. September dieses Jahres zu einem beispiellosen Drohnenangriff von jenseits der östlichen Grenze. Ein Teil davon wurde zerstört, der Rest stürzte aufgrund von Antriebsausfall (Treibstoffmangel) ab. Beim Überfliegen der Luftgrenze hätte das Warn- und Alarmsystem ausgelöst werden müssen, doch leider verhinderte, ähnlich wie an der Westgrenze, das Fehlen von Diensthabenden das sofortige Einschalten der Sirenen. Vgl. Rosyjskie drony nad Polską. Najnowsze informacje z ostatnich godzin (podsumowanie) (Russische Drohnen über Polen. Aktuelle Informationen aus den letzten Stunden (Zusammenfassung)), onet.pl, 11.09.2025, https://wiadomosci.onet.pl/kraj/rosyjskie-drony-nad-polska-najnowsze-informacje-z-ostatnich-godzin-podsumowanie/47hhlx8 (Zugang am: 11.09.2025).

Jahrzehnten seit Inkrafttreten des Gesetzes und mehreren Novellierungen regelt es immer noch viele Fragen nicht (die letzte Änderung erfolgte 2024). Aus Ankündigungen geht hervor, dass der nächste Novellierungsumfang die Umsetzung der NIS2-Richtlinie und der CER.

Das Gesetz vom 5. Dezember 2024 über den Schutz der Bevölkerung und den Zivilschutz ergänzte das Gesetz über das Krisenmanagement[64]. Es füllte die Lücke, die nach der Verabschiedung des Gesetzes vom 11. März 2022 über die Verteidigung des Vaterlandes[65] entstanden war, und hob gleichzeitig das Gesetz vom 21. November 1967 über die allgemeine Wehrpflicht in der Republik Polen auf. Der Bereich des Zivilschutzes wurde durch das Gesetz über die allgemeine Wehrpflicht der Republik Polen[66] und die auf der Grundlage dieses Gesetzes erlassenen Durchführungsbestimmungen geregelt, während das Gesetz über die Verteidigung des Vaterlandes diese Fragen überhaupt nicht regelte. Unter diesen Umständen wurde die Wiedereinführung des Zivilschutzes in das Rechtssystem dringend erforderlich. Als Argument für die Beschleunigung der Arbeiten wurde natürlich auch der Krieg in der Ukraine und dessen Nähe zu den polnischen Grenzen und damit dessen Einfluss auf das Sicherheitsgefühl der Bewohner der östlichen Grenzgebiete des Landes angeführt.

Das Gesetz über den Bevölkerungsschutz und den Zivilschutz ergänzt das Krisenmanagement, da es dieselben Schutzakteure betrifft. Seine Aufgabe besteht darin, die bestehenden zivilen Strukturen und Systeme zu nutzen, die darauf ausgerichtet sind, das Leben und die Gesundheit der Bevölkerung bei Gefahren, einschließlich Krisensituationen, sowie bei der Verhängung des Ausnahmezustands und im Kriegsfall zu schützen.

Es legt Folgendes fest:

1. Aufgaben des Bevölkerungsschutzes und des Zivilschutzes,
2. Behörden und Stellen, die Aufgaben des Bevölkerungsschutzes und des Zivilschutzes wahrnehmen,
3. Grundsätze für die Planung des Bevölkerungsschutzes und des Zivilschutzes,
4. Grundsätze für die Funktionsweise von Systemen zur Erkennung von Gefahren sowie zur Benachrichtigung, Warnung und Alarmierung bei Gefahren,
5. die Grundsätze für die Nutzung und Erfassung sowie die technischen Bedingungen von Objekten des kollektiven Schutzes,
6. die Grundsätze für die Funktionsweise und Organisation des Zivilschutzes sowie die Art und Weise der Einberufung von Personal für den Zivilschutz,
7. die Grundsätze für die Finanzierung des Katastrophenschutzes und des Zivilschutzes.

64 Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Gesetz vom 5. Dezember 2024 über den Bevölkerungsschutz und den Zivilschutz), GBl. 2024 Pos. 1907, (Zugang am: 06.10.2025).

65 Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Gesetz vom 11. März 2022 über die Verteidigung des Vaterlandes), GBl. 2022 POs. 655, (Zugang am: 06.10.2025).

66 Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Gesetz vom 21. November 1967 über die allgemeine Wehrpflicht zur Verteidigung der Republik Polen), GBl. 1967 Nr. 44 Pos. 220, (Zugang am: 06.10.2025).

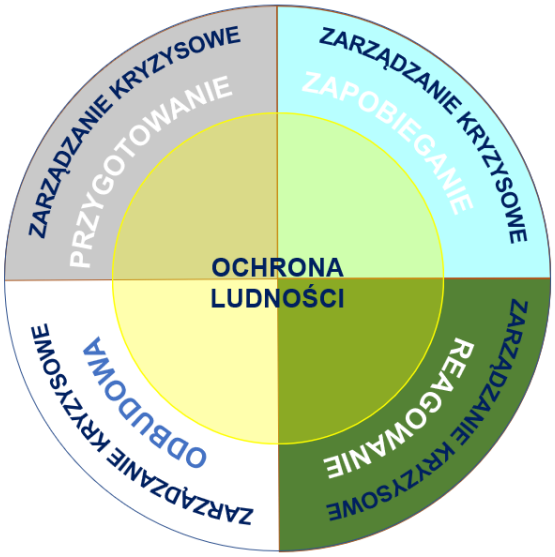
Das Gesetz definiert den Bevölkerungsschutz als „ein System, das aus öffentlichen Verwaltungsbehörden besteht, die Aufgaben zur Gewährleistung der Sicherheit der Bevölkerung durch den Schutz des Lebens und der Gesundheit von Menschen, von Eigentum, von für die Befriedigung der Lebensbedürfnisse notwendiger Infrastruktur, von Kulturgütern und der Umwelt in Gefahrensituationen, von den diese Aufgaben wahrnehmenden Stellen sowie von den zur Erfüllung dieser Aufgaben bestimmten Kräften und Mitteln wahrnehmen". Jede Behörde auf jeder Ebene hat festgelegte Aufgaben, aber auch Kompetenzen gegenüber den Behörden der unteren und höheren Ebenen. Beispielsweise wurden dem Gemeindevorsteher (Bürgermeister, Stadtpräsident) in Art. 10 Abs. 1 des Gesetzes über den Bevölkerungsschutz und den Zivilschutz unter anderem folgende Aufgaben übertragen:

1. Leitung und Koordinierung der Maßnahmen von Einrichtungen im Bereich des Bevölkerungsschutzes und des Zivilschutzes auf dem Gebiet der Gemeinde,
2. Organisation der Zusammenarbeit zwischen den Einrichtungen des Bevölkerungsschutzes und des Zivilschutzes im Gemeindegebiet,
3. Schaffung und Aufrechterhaltung von Ressourcen für den Bevölkerungsschutz und der für die Erfüllung der Aufgaben des Bevölkerungsschutzes und des Zivilschutzes sowie der Wasserversorgung erforderlichen Infrastruktur im Gemeindegebiet,
4. Abstimmung mit dem Kreis- (Stadt-) Kommandanten der Staatlichen Feuerwehr über die Ressourcen der Gemeinde, die für die Zusammenarbeit im Kreisbereich vorgesehen sind,
5. Leistung von Soforthilfe mit Hilfe von Katastrophenschutzstellen im Gemeindegebiet,
6. Planung und Organisation von Schulungen, Übungen und anderen Formen der Ausbildung im Bereich des Katastrophenschutzes und der Zivilverteidigung sowie Unterstützung von Bildungsprogrammen, die auf die Vorbereitung auf potenzielle Gefahren im Gebiet der Gemeinde abzielen,
7. Benachrichtigung, Warnung und Alarmierung der Bevölkerung über Gefahren im Gebiet der Gemeinde;
8. Aufrechterhaltung der Bereitschaft der kommunalen Elemente der Gefahrenerkennungssysteme sowie der Systeme zur Benachrichtigung, Warnung und Alarmierung bei Gefahren[67].

Ergänzt wird das Gesetz durch das daraus resultierende Programm für Bevölkerungsschutz und Zivilverteidigung, das alle vier Jahre vom Ministerrat verabschiedet wird, mit Ausnahme des ersten Programms, das für die Jahre 2025 und 2026 gilt. Diese neue Rechtskonstruktion, zu der auch das Programm für Bevölkerungsschutz und Zivilschutz gehört, schafft potenzielle Voraussetzungen für die Organisation der Zusammenarbeit im Rahmen der Krisenmanagementstrukturen der beiden Städte.

Abbildung 2. Zusammenhang zwischen Krisenmanagement, Katastrophenschutz und Zivilschutz

67 Ibidem, S. 5-6.



OCHRONA LUDNOŚCI → Bevölkerungsschutz
PRZYGOTOWANIE → Vorbereitung
ZAPOBIEGANIE → Vorbeugung
REAGOWANIE → Reaktion
ODBU DOWA → Wiederaufbau
ZARZĄDZANIE KRYZYSOWE → Krisenmanagemen

Quelle: eigene Ausarbeitung.

Das Gesetz über den Bevölkerungsschutz und den Zivilschutz präzisiert die Bestimmungen des Gesetzes über das Krisenmanagement und legt größeren Wert auf die Mitverantwortung der Gemeindevorsteher und der Bürger selbst für die Sicherheit der Einwohner. Zu diesem Zweck werden die Behörden für Bevölkerungsschutz und Zivilschutz auf der untersten Ebene verpflichtet, angemessene Vorräte an Ressourcen anzulegen, die in einer Krisensituation für die Bereitstellung von Soforthilfe und humanitärer Hilfe erforderlich sind. Diese Ressourcen umfassen insbesondere Wasservorräte und Mittel zu deren Lagerung, Transport und Aufbereitung, Ersatzenergiequellen und Brennstoffe, Kleidung, Lebensmittelvorräte, Sanitär- und Hygieneartikel, Arzneimittel und Medizinprodukte sowie stationäre und mobile Notunterkünfte. Daraus ergibt sich die Notwendigkeit, Lager einzurichten und darin Ressourcen für den Katastrophenschutz zu sammeln, die für mindestens drei Tage der Gefahrensituation Folgendes gewährleisten:

1. Zugang zu Wasser und Nahrungsmitteln,
2. Zugang zu Medikamenten und Erste-Hilfe-Leistungen, qualifizierter Erster Hilfe und Gesundheitsversorgung,
3. Unterstützung bei der Durchführung von Rettungsmaßnahmen,
4. Benachrichtigung, Warnung und Alarmierung der Bevölkerung,
5. Aufrechterhaltung der öffentlichen Sicherheit und Ordnung,

6. Funktionieren von Einrichtungen des kollektiven Schutzes[68].

Derzeit erleben wir im Zusammenhang mit der Umsetzung des Gesetzes über den Bevölkerungsschutz und den Zivilschutz Veränderungen im Bereich des Krisenmanagements, was auch als guter Zeitpunkt für die Verbesserung der grenzüberschreitenden Zusammenarbeit in Krisensituationen angesehen werden kann.

Schlussfolgerungen und Empfehlungen

Die vorgestellten Änderungen veranlassen zu gemeinsamen Empfehlungen für beide Seiten der Doppelstadt. Das Gesetz über den Bevölkerungsschutz und den Zivilschutz führt neue Lösungen im Bereich der Warnung und Alarmierung ein.[69] Es legt die Grundsätze für die Organisation und Durchführung von Evakuierungen der Einwohner fest, die durch verschiedene Gefahren und Umstände verursacht werden, die ihre Gesundheit oder ihr Eigentum gefährden. Es legt den Schwerpunkt auf die Schaffung von Lagern für Zivilschutzressourcen, die Vorräte für die Bevölkerung in einem bestimmten Gebiet für einen Zeitraum von mindestens 72 Stunden enthalten. Es wäre sinnvoll, bereits in dieser Phase Vereinbarungen zwischen den Krisenmanagementstrukturen hinsichtlich der Zusammenarbeit und der Grundsätze der gegenseitigen Unterstützung in bestimmten Gefahrensituationen zu treffen oder zumindest zu beginnen. Ausgangspunkt kann ein gemeinsamer und abgestimmter Katalog von Gefahren sowie gegenseitige zwischenmenschliche Kontakte sein, die schnelle, informelle Kanäle für den Austausch von Informationen, Erfahrungen und technischen Lösungen schaffen. Das Jahr 2025 und die Erfahrungen, die die Krisenmanagementstrukturen der beiden Städte in mehr als zwei Jahrzehnten der Geltungsdauer des Abkommens zwischen dem Minister für Inneres und Verwaltung der Republik Polen und dem Ministerium für Inneres des Landes Brandenburg über gegenseitige Hilfe bei Katastrophen, Naturkatastrophen und anderen schweren Unfällen, das am 18. Juli 2002 in Słubice ausgearbeitet und unterzeichnet wurde, veranlassen dazu, einen neuen Inhalt auszuarbeiten, in dem es sich lohnt, die Errungenschaften neuer Technologien zu nutzen.

68 Ibidem, S. 18-19.

69 Die Ergebnisse, d. h. das neue Erkennungs-, Warn- und Alarmsystem, werden frühestens in einigen Monaten vorliegen.

Dariusz DYMEK, Mikołaj TOMASZYK, Łukasz ŻYSZKIEWICZ

KAPITEL VII. KRISENMANAGEMENT IN GRENZÜBERSCHREITENDEN REGIONEN – ALLGEMEINE BEMERKUNGEN

Der Katalog der Gefahren, die das Gebiet der Doppelstadt Słubice-Frankfurt (Oder) betreffen, ist identisch, während die Herangehensweise an die Minimierung oder Beseitigung dieser Gefahren unterschiedlich ist. Diese Unterschiede zeigen sich bereits auf der Ebene der Rechtsgrundlagen für die Funktionsweise der für Krisenmaßnahmen zuständigen Strukturen.

In Deutschland gibt es kein einheitliches Gesetz zur Krisenbewältigung, wie es in Polen geregelt ist (siehe Kapitel VI dieser Studie). Es gibt auch keine einheitliche Definition einer Krisensituation, also des Zeitpunkts, zu dem die Krisenbewältigungsstrukturen in die Reaktionsphase eintreten.

Die allgemeine Definition einer Krisensituation in Deutschland (basierend auf Regierungsdokumenten und Krisenmanagementstrategien) lautet: „Eine Krisensituation ist ein außergewöhnliches Ereignis, das das Funktionieren grundlegender sozialer, politischer, wirtschaftlicher oder ökologischer Strukturen erheblich stört oder gefährdet und koordinierte Maßnahmen der öffentlichen Verwaltung, der Rettungsdienste und anderer für die Sicherheit zuständiger Stellen erfordert.“[70]. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) – BBK) den Begriff Krisenmanagement für „alle Maßnahmen zur Prävention, Vorsorge, Reaktion und Wiederherstellung nach Ereignissen, die Leben, Gesundheit oder kritische Infrastrukturen der Gesellschaft gefährden”[71]. Eine weitere Definition findet sich im Zivilschutzgesetz oder im BSI-Gesetz, wonach „eine Krise auch als eine Situation verstanden werden kann, die über die Möglichkeiten des täglichen Handelns der Verwaltungsstrukturen hinausgeht

70 Das BBK entwickelt die konzeptionellen Grundlagen des Krisenmanagements durch die Auswertung realer Ereignisse und Katastrophenübungen und initiiert und fördert Forschungsprojekte, um eine kontinuierliche Überprüfung und Anpassung der Verfahren und Strukturen des Krisenmanagements zu ermöglichen. Auf dieser Grundlage erarbeitet das BBK Konzepte, Leitlinien und methodische Ansätze zur Optimierung des Krisenmanagements in den Bundes- und Landesbehörden sowie der übergeordneten Zusammenarbeit zwischen ihnen. Es ist zu beachten, dass sich diese Begriffe auf zwei Elemente beziehen und keine Synonyme sind, sodass ihre Gegenüberstellung unzulässig ist. Die Definition auf Bundesebene ist sehr allgemein gehalten, da dieser Zuständigkeitsbereich im deutschen Recht der Gerichtsbarkeit der Landesregierungen überlassen bleibt. Jedes Bundesland hat diese Fragen in den in seinem Gebiet geltenden Gesetzen präzisiert. Für Frankfurt (Oder) gilt das BbgBKG, das die Definition des Begriffs enthält. Um jedoch einen breiteren Kontext zu skizzieren, sei erwähnt, dass für die deutsch-polnische Zusammenarbeit die Rechtsvorschriften im Bereich Katastrophenschutz und Brandschutz für die Grenzgebiete auf deutscher Seite, die für jedes Bundesland, d. h. für Mecklenburg-Vorpommern, Brandenburg und Sachsen, was wiederum die Beteiligung der für diesen Bereich zuständigen Innenministerien dieser drei Bundesländer am Prozess der Ausarbeitung eines deutsch-polnischen Abkommens im Bereich des Katastrophenschutzes erforderlich macht. Es gibt zwei mögliche Lösungen für dieses Problem: Die erste besteht darin, dass die Bundesregierung in Absprache mit allen Bundesländern eine gemeinsame Definition der Begriffe dieses Bereichs erstellt, was jedoch leider das Problem der uneinheitlichen weiteren Lösungen in den einzelnen Bundesländern nicht löst. Das zweite Modell sieht die Einführung von Regelungen auf EU-Ebene vor, die die Vorschriften in der gesamten Europäischen Union vereinheitlichen und deren Umsetzung auf Ebene der Mitgliedstaaten erforderlich machen.

71 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Krisenmanagement, https://www.bbk.bund.de/DE/Themen/Krisenmanagement/krisenmanagement_node.html (Zugang am: 06.09.2025).

und die Aktivierung außerordentlicher Mechanismen des Managements und der sektorübergreifenden Zusammenarbeit erfordert"[72].

Die Struktur und Form des Katastrophenschutzes in Frankfurt (Oder) und weitgehend auch die Zusammenarbeit mit Słubice in diesem Bereich werden durch die Tatsache bestimmt, dass es sich um eine kreisfreie Stadt handelt. Die Stadtverwaltung ist für den Zivilschutz, das Krisenmanagement und den Brandschutz in ihrem Gebiet zuständig. Das Krisenmanagementmodell wird hingegen durch die Staatsform beeinflusst. Deutschland ist ein föderaler Staat, weshalb das Katastrophenschutzsystem eine grundlegend andere Struktur hat als in Polen.

Gemäß dem Brandenburgischen Brand- und Katastrophenschutzgesetz (BbgBKG) ist Frankfurt (Oder) die untere Katastrophenschutzbehörde.[73]. Es ist sowohl für den vorbeugenden Katastrophenschutz als auch für die Bekämpfung von Katastrophen und deren Folgen zuständig.

Die Behörden von Frankfurt (Oder) haben die Aufgabe, die notwendigen Vorbereitungsmaßnahmen zu treffen, um einen wirksamen Katastrophenschutz zu gewährleisten. Zu diesen Maßnahmen gehören insbesondere:

1. Einrichtung einer Leitung für den Katastrophenschutz zur Unterstützung der allgemeinen Leitung zusammen mit einem Stab für den Katastrophenschutz,
2. Errichtung und Unterhaltung von Einrichtungen und Objekten zum Katastrophenschutz, insbesondere von Lagern zum Katastrophenschutz,
3. Durchführung von Schulungen und Fortbildungskursen für Mitglieder des Katastrophenschutzes, einschließlich des Stabspersonals,
4. Ausarbeitung und Aktualisierung von Katastrophenschutzplänen sowie
5. Durchführung von Katastrophenschutzübungen[74].

In Bezug auf diese Maßnahmen sollten die zur Umsetzung dieser Maßnahmen ergriffenen Aufgaben in der Praxis darauf hinauslaufen, dass:

- die Leitung nicht nur aus Mitarbeitern der Katastrophenschutzbehörden, sondern auch aus Vertretern von Hilfsbehörden und -institutionen besteht (das Thema der Hilfsorganisationen wird im weiteren Verlauf des Kapitels näher erläutert) (ad. 1),

72 Ibidem; Zivilschutz- und Katastrophenhilfegesetz vom 25. März 1997 (BGBl. I S. 726), das zuletzt durch Artikel 144 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, https://www.gesetze-im-internet.de/zsg/ZSKG.pdf (dostęp: 05.10.2025); BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist, https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf (Zugang am: 05.10.2025).

73 Gesetz über den Brandschutz, die Hilfeleistung und den Katastrophenschutz des Landes Brandenburg (Brandenburgisches Brand- und Katastrophenschutzgesetz – BbgBKG) vom 24. Mai 2004 zuletzt geändert durch Artikel 9 des Gesetzes vom 5. März 2024, część 1, § 2, pkt 2, https://bravors.brandenburg.de/gesetze/bbgbkg (Zugang am: 05.10.2025).

74 Ibidem, Teil 4, Kap. 1, § 37.

- die Pläne aktualisiert werden und eine Risikoanalyse für die Stadt sowie spezielle Pläne für die einzelnen in der Analyse erkannten Gefahren enthalten (ad. 4)[75],

- Die Übungen hatten zum Ziel, das System auf einem angemessenen Leistungs- und Bereitschaftsniveau zu halten. In der Verordnung zu dem oben genannten Gesetz sind fünf Arten von geplanten Übungen festgelegt, nämlich:

  a) geplante Übungen,

  b) Alarmübungen,

  c) Marschübungen,

  d) Stabsübungen,

  e) vollständige Übungen (ad. 5)[76].

Diese Übungen sollten für die ersten vier Arten in Abständen von höchstens zwei Jahren stattfinden. Für vollständige Übungen kann dieser Abstand maximal fünf Jahre betragen. Eine Ausnahme ist für reale Ereignisse vorgesehen, die grundsätzlich als absolvierte Übungen für die an der Aktion beteiligten Einheiten gelten können[77]. Wenn beispielsweise bei einer Hochwasseraktion alle Katastrophenschutzkräfte eingesetzt wurden, müssen die nächsten vollständigen Übungen innerhalb von fünf Jahren stattfinden usw.

Bei der Bekämpfung von Katastrophen und deren Folgen stellt die untergeordnete Katastrophenschutzbehörde, also die Stadt Frankfurt (Oder), das Auftreten und das Ende eines Katastrophenzustandes fest, in dem Katastrophenschutzkräfte und -mittel eingesetzt werden müssen. . Diese Information muss unverzüglich im betroffenen Gebiet bekannt gegeben, an die benachbarten Katastrophenschutzbehörden und an die oberste Katastrophenschutzbehörde, d. h. das Ministerium für Inneres und Kultur des Landes Brandenburg, weitergeleitet werden[78]. In einer solchen Situation stehen auch die Kräfte und Mittel des Bundes zur Verfügung, die für den Zivilschutz bestimmt sind[79]. Der Zivilschutz und der Katastrophenschutz selbst fallen in den Zuständigkeitsbereich der Bundesregierung, was sich aus dem Grundgesetz für die Bundesrepublik Deutschland ergibt[80].

Ein besonders wichtiger Bestandteil des Krisenmanagements ist die Arbeit des Krisenstabs, der von der Stadt Frankfurt (Oder) oder dem für die Art der Gefahr oder Katastrophe zuständigen Ministerium des Landes Brandenburg einberufen werden kann. Grundsätzlich sind zwei Modelle für Krisenstäbe im Katastrophenschutz vorgesehen. Das erste Modell sieht eine Trennung zwischen Verwaltungsstab und

75 Es besteht auch die Verpflichtung, separate Pläne für einzelne Sonderobjekte zu erstellen, jedoch gibt es derzeit in Frankfurt (Oder) keine derart klassifizierten Objekte.

76 Verordnung über die Einheiten und Einrichtungen des Katastrophenschutzes (Katastrophenschutzverordnung – KatSV) vom 17. Oktober 2012 (GVBl.II/12, [Nr. 87]) zuletzt geändert durch Verordnung vom 16. Dezember 2021 (GVBl.II/21, [Nr. 102], S. ber. GVBl.II/22 [Nr. 31]), § 5, pkt 3, https://bravors.brandenburg.de/verordnungen/katsv (Zugang am: 05.10.2025).

77 Ibidem, § 5, Nr. 5.

78 Gesetz über den Brandschutz, die Hilfeleistung…, op. cit., Kap. 2, § 42.

79 Zivilschutz- und Katastrophenhilfegesetz vom 25. März 1997…, op. cit., § 12.

80 Grundgesetz, Art. 73 Nr. 1, https://www.btg-bestellservice.de/pdf/80205000.pdf (Zugang am: 05.10.2025).

Führungsstab vor. Im zweiten Modell gibt es einen gemeinsamen Stab, der auf beiden Komponenten basiert[81]. Beide Modelle haben ihre Vor- und Nachteile, und ihre Umsetzung hängt von der jeweiligen Situation und ihrer Dynamik ab.

An der Spitze des Stabes steht der Hauptverwaltungsbeamte (HVB). Diese Funktion im Katastrophenschutz kann nach Absolvierung eines speziellen Kurses ausgeübt werden (ähnlich wie derzeit in Polen). Tatsächlich hat der HVB das Kommando, während der Stab eine unterstützende Funktion hat. Über ihn werden auch die direkten Maßnahmen und alle notwendigen Aktivitäten koordiniert. Der Stab besteht in der Regel aus folgenden Personen:

- Vertreter der Behörde für Sicherheit und Ordnung (vereinfacht gesagt, das Äquivalent zur polnischen Stadtpolizei),
- Verbindungsmann zum Kommandostab (im getrennten Modell),
- Vertreter des Katastrophenschutzes,
- Vertreter des Gesundheitsamtes (das Äquivalent zum polnischen Sanepid),
- Vertreter des Umweltamtes,
- Vertreter der Sozialhilfe,
- Koordinierungsgruppe des Verwaltungsstabs (im getrennten Modell),
- Person, die für die Information der Bevölkerung und die Zusammenarbeit mit den Medien zuständig ist,
- Polizei.

Darüber hinaus können Experten, Berater, Vertreter von Unternehmen und Institutionen, die für die Arbeit des Stabes erforderlich sind, sowie Vertreter einzelner Abteilungen der Stadtverwaltung, die aus Sicht des HVB für die Bekämpfung der Katastrophe benötigt werden, in den Stab berufen werden.

Der Katastrophenschutzstab muss die definierten Funktionen S1 bis S4 zuweisen. Die Funktionen S5 und S6 galten bisher als optional, d. h. sie sollten bei Bedarf zugewiesen werden. Derzeit bleiben die Funktionen S5 und S6 nur bei erheblichem Personalmangel unbesetzt. Die einzelnen Buchstaben S (von Sachgebiet) stehen für folgende Funktionen:

- S1 – Personal und interner Dienst: Verantwortlich für das für die Durchführung der Aktion und den Betrieb des Stabes erforderliche Personal. Zu dieser Funktion gehören unter anderem die

[81] H. Georsch, A. Kling (red,), Kompetent und rechtssicher handeln: Einführung in den Bevölkerungsschutz, Walhalla Fachverlag, Regensburg 2024, S. 253.

Alarmierung und Überwachung des für den Betrieb des Stabes und die Durchführung der Aktion erforderlichen Personals,

- S2 – Situation und Dokumentation: Verantwortlich für die Situationserkennung im Stab. Nimmt Informationen entgegen, die den Stab erreichen, erfasst sie, verarbeitet sie so, dass sie optimal präsentiert werden können, und liefert gleichzeitig die notwendigen Informationen, damit der HVB und andere Stabsmitglieder in den übrigen Teilen des Stabs Entscheidungen treffen können,

- S3 – Verwendung: In diesem Bereich werden Ziele, Prioritäten und operative Aufgaben zusammen mit Anweisungen zu deren Umsetzung festgelegt. S3 kann den Einsatzbereich in Abschnitte unterteilen. Allgemein gesagt ist er für die Taktik verantwortlich und überwacht gleichzeitig den Ablauf der Aktion und die Durchführung ihrer einzelnen Elemente. Dies ist ein Bereich von entscheidender Bedeutung und in der Regel mit der größten Arbeitsbelastung verbunden,

- S4 – Versorgung und Logistik: Verantwortlich für die gesamte Versorgung und Logistik, nicht nur im Zusammenhang mit den unmittelbar für die Katastrophenbekämpfung erforderlichen Kräften und Mitteln, sondern auch für alles, was in der jeweiligen Situation im Rahmen des Katastrophenschutzes zur Gewährleistung der Sicherheit der Bevölkerung erforderlich ist,

- S5 – Pressesprecher: Seine Aufgabe ist es, die Medien, einschließlich der sozialen Medien, zu analysieren, um wichtige Informationen für die beteiligten Kräfte zu gewinnen. Er informiert die Bevölkerung über die Lage und die ergriffenen Maßnahmen, soll aber vor allem ihr Verhalten in kontrollierter Weise beeinflussen und so die Bewältigung der Krisensituation erleichtern,

- S6 – Informationsfluss und Kommunikation: Aufgabe dieses Bereichs ist es, einen reibungslosen Informationsfluss und die Kommunikation zwischen allen an der Katastrophenbekämpfung beteiligten Kräften sicherzustellen[82].

In Frankfurt (Oder) ist die Feuerwehr die erste Verteidigungslinie gegen Gefahren im nichtpolizeilichen Bereich. Sie besteht aus einer Berufs- und einer Freiwilligen Feuerwehr. Ein integraler Bestandteil der Berufsfeuerwehr ist der Rettungsdienst. Sowohl der Brandschutz als auch die technische Hilfe und der Rettungsdienst gehören zu den Aufgaben der Stadt Frankfurt (Oder)[83]. Im deutschen System gibt es keine vertikale Struktur mit einem hierarchisch aufgebauten Hauptkommandoelement, stattdessen gibt es vertikale Abhängigkeiten. In Frankfurt (Oder) untersteht die Feuerwehr dem Oberbürgermeister, der ihr oberster Vorgesetzter ist. Alle Feuerwehren sind gleichberechtigt und unterstehen ebenfalls dem zuständigen Landkreis oder der kreisfreien Stadt, ohne dass eine gegenseitige Unterordnung besteht.

82 FwDV 100, Feuerwehr-Dienstvorschrift 100, marzec 1999, s. 12-13, 48, 51 https://www.idf.nrw.de/dokumente/wir-ueber-uns/aufgaben-des-idf/fwdv100.pdf (dostęp: 05.10.2025).

83 Gesetz über den Brandschutz, die Hilfeleistung…, op. cit.; Gesetz über den Rettungsdienst im Land Brandenburg (Brandenburgisches Rettungsdienstgesetz - BbgRettG) vom 14. Juli 2008 (GVBl.I/08, [Nr. 10], S.186) zuletzt geändert durch Artikel 4 des Gesetzes vom 20. Juni 2024 (GVBl.I/24, [Nr. 28], S.8), § 6, https://bravors.brandenburg.de/gesetze/bbgrettg (dostęp: 05.10.2025).

Diese Situation ermöglicht eine wesentlich flexiblere Nutzung dieser Kräfte und Mittel in Krisensituationen durch die Stadtverwaltung.

Besondere Aufmerksamkeit verdient die Präsenz von Hilfsorganisationen im Katastrophenschutzsystem in Deutschland, die in Polen in dieser Form völlig unbekannt ist. In Frankfurt (Oder) sind drei Organisationen mit dem Status einer Hilfsorganisation tätig, und zwar:

- DRK (Deutsches Rotes Kreuz)[84],
- DLRG (Deutsche Lebens-Rettungs-Gesellschaft) und
- ASB (Arbeiter-Samariter-Bund).

Die ersten beiden verfügen über Fahrzeuge und Ausrüstung für den Katastrophenschutz und die Zivilverteidigung, während die dritte bei Bedarf ein medizinisches Team entsendet. Die Stadt hat das Recht, sie in dem von ihr als notwendig erachteten Umfang in das Katastrophenschutzsystem einzubeziehen. Die Zusammenarbeit umfasst die Verpflichtung, das erforderliche Personal bereitzustellen, es auszubilden und die Einsatzbereitschaft der übergebenen Einheiten aufrechtzuerhalten. Bei Einsätzen, Übungen und Schulungen, die von der Stadt angeordnet wurden, handeln die Einheiten und Institutionen, die sich mit dem Schutz der Bevölkerung befassen, im Auftrag der Stadt.

Der Katastrophenschutz im Land Brandenburg sieht die Einrichtung von sieben Fachdiensten vor, nämlich:

- Leitung,
- Brandschutz,
- medizinischer Dienst,
- Betreuungsdienst,
- Schutz vor gefährlichen Stoffen,
- Rettung/Reparatur, einschließlich Gefahren im Zusammenhang mit Wasser, und
- Versorgung[85].

In Frankfurt (Oder) wurde dieser Effekt durch den Einsatz sowohl von Hilfsorganisationen als auch der Feuerwehr erreicht, wodurch eine schnelle Anpassung der Struktur an die Aufgaben und eine möglichst effiziente Nutzung der verfügbaren Kräfte und Mittel ermöglicht wurde.

84 Najliczniejsza grupa w ochronie przed katastrofami (Katastrophenschutz).

85 Verordnung über die Einheiten und Einrichtungen des Katastrophenschutzes…, op. cit., § 2, Nr. 1.

Ein wichtiger Bestandteil des Katastrophenschutzes in Deutschland ist das 1950 gegründete Technische Hilfswerk (THW), das sich im Wesentlichen mit drei Bereichen befasst. Der erste Bereich ist die technische Hilfe im Katastrophenschutz (dies liegt in der Zuständigkeit der Bundesbehörden, denen das THW untersteht). Der zweite Bereich ist die technische Hilfe im Ausland auf Anordnung der Bundesbehörden. Der dritte Bereich ist die technische Hilfe bei Katastrophen und Notfällen auf Antrag der zuständigen Behörden. Zuletzt wurde das THW in Frankfurt (Oder) im Jahr 2024 bei der Errichtung einer Spundwand eingesetzt.

Es ist zu beachten, dass gemäß dem Gesetz über Brandschutz, Hilfe und Katastrophenschutz des Landes Brandenburg (BbgBKG) der Bevölkerung eine Reihe von Pflichten auferlegt wurden:

- Gefahrenverhütung,
- Meldepflicht,
- Hilfeleistungspflichten,
- Pflichten von Eigentümern und Besitzern von Immobilien im Bereich der Brandverhütung,
- Unterstützungspflichten von Eigentümern und Besitzern von Immobilien[86].

Die oben genannten rechtlichen Rahmenbedingungen und die daraus resultierenden organisatorischen Rahmenbedingungen wirken sich auf die Strukturen aus, die in jeder der benachbarten Regionen unterschiedlich sind. Dies ändert jedoch nichts an der Tatsache, dass auf der untersten Ebene Krisenstäbe funktionieren (natürlich in dem Moment, in dem eine Gefahr bekämpft wird) und ihre Tätigkeit auf zuvor festgelegten Plänen und Verfahren basiert. Bei jeder Gefahr muss ein Warn- und Alarmverfahren eingeleitet werden, und da viele Gefahren, insbesondere Naturgefahren (Luftverschmutzung, Flussverschmutzung, heftige Niederschlagsereignisse, Epidemien usw.), keine Grenzen kennen und meist in beiden Städten gleichzeitig oder in kurzen Zeitabständen auftreten, ist es sinnvoll, die Krisenmaßnahmen zu synchronisieren. In diesem Zusammenhang ist es sinnvoll, IT-Tools einzusetzen, die den Informationsaustausch verbessern und die Effizienz der Zusammenarbeit steigern.

Laut Anna Dziadkiewicz und Marian Żuber „besteht die Zusammenarbeit im Krisenmanagement in der Abstimmung von Ziel, Zeitpunkt und Ort des Einsatzes der Kräfte und Mittel, über die alle an den Maßnahmen zur Bewältigung der Krisensituation beteiligten Akteure verfügen. Diese Maßnahmen werden mit dem Ziel durchgeführt, eine bestimmte Aufgabe bestmöglich zu erfüllen, nämlich die Minimierung der schädlichen Auswirkungen der entstandenen Gefahr auf die Bevölkerung, das Eigentum und die Umwelt. Der Kern einer solchen Maßnahme ist die Notwendigkeit, gemeinsame Maßnahmen zu organisieren, die Bemühungen zu integrieren und zu koordinieren, die durch ein gemeinsames Ziel und den Willen zu dessen Erreichung verbunden sind. Daher ist es so wichtig, dass alle ergriffenen Maßnahmen so konkretisiert werden, dass alle Beteiligten wissen, welche Rolle sie spielen und welche konkreten Aufgaben sie ausführen. Die Erfüllung dieser Bedingung kann die

86 Gesetz über den Brandschutz, die Hilfeleistung…, op. cit.

Gewissheit geben, dass diese Maßnahmen die beabsichtigte Wirkung erzielen[87]. Eine solche Zusammenarbeit führt uns zu integrierten IT-Tools, die dank ihrer Funktionalität eine effektive Zusammenarbeit der Dienste beider Städte gewährleisten könnten.

In einer Umfrage antworteten 61 % der Befragten auf die Frage „Bitte geben Sie anhand Ihrer Berufserfahrung an, welche Hindernisse in der grenzüberschreitenden Zusammenarbeit die Erfüllung Ihrer beruflichen Pflichten und Aufgaben am meisten erschweren. Bitte wählen Sie maximal 5 Hindernisse aus", gaben 61 % der Befragten an, dass die Struktur der Zuständigkeitsverteilung zwischen Behörden und Verwaltungen nicht an die grenzüberschreitenden Gegebenheiten angepasst sei, fast 67 % nannten das Fehlen gemeinsamer Pläne und Verfahren für Krisensituationen bei grenzüberschreitenden Notfällen, 44 % nannten Schwierigkeiten in der operativen Kommunikation (Fehlen einer gemeinsamen Arbeitssprache) und 39 % die mangelnde Interoperabilität der IT-Systeme (Fehlen gemeinsamer Datenbanken). Die Ergebnisse zeigen, dass über die Richtung der Veränderungen hinsichtlich der Interoperabilität der Krisenmanagementstrukturen auf beiden Seiten der Oder nachgedacht werden muss. Während im Bereich der Strukturen wenig geändert werden kann, da jedes Land seine eigenen bewährten Lösungen und Strukturen hat, können solche Änderungen im Bereich des Informationsaustauschs bereits vorgeschlagen werden.

Derzeit gibt es auf dem polnischen Markt Angebote verschiedener Anbieter, die zuverlässige und sichere Kommunikation in kritischen Situationen gewährleisten. Diese ermöglichen unter anderem:

- sofortige Kommunikation,
- drahtlose Verbindung,
- cybersichere Übermittlung von Nachrichten,
- Interoperabilität,
- Sprach- und Videokonferenzen,
- Priorisierung von Verbindungen im Modul der integrierten Kommunikation mehrerer Dienste,
- fortschrittliche Kartierung,
- Aufrechterhaltung der Kommunikation bei Überlastung des Mobilfunknetzes,
- Kommunikation per Chat mit der Möglichkeit, Dateien zu übertragen,
- Erfassung und Analyse von Daten aus Messgeräten und anderen.

87 A. Dziadkiewicz, M. Żuber, Zusammenarbeit von Behörden, Inspektionen und Wachdiensten auf Kreisebene in Notfällen, „Historia i Polityka" nr 23 (30), 2018, s. 78.

Ein wesentlicher Vorteil integrierter Kommunikationssysteme ist die Möglichkeit, die Kommunikationsmittel verschiedener Dienste und öffentlicher Verwaltungen zu integrieren. Diese Systeme sind eine gute Lösung für Rettungsdienste, Zivilschutz, Feuerwehr, Polizei, Kommunalverwaltung und andere wichtige Einrichtungen, z. B. Gas- oder Energieversorger. Aus grenzüberschreitender Sicht stellt jedoch die Leitung von Einsätzen, an denen Dienste aus zwei oder mehr Ländern beteiligt sind, eine kommunikative Herausforderung dar.

Die Ergebnisse der Untersuchungen zeigen, dass es im polnischen Krisenmanagement kein IT-System gibt, das das Krisenmanagement unterstützt. Bereits bei der Aufforderung, drei der im Land eingesetzten Systeme zur Unterstützung der Krisenbewältigung/des Krisenmanagements zu nennen, wird deutlich, dass die bekannteste IT-Lösung unter den Beamten (Feuerwehrleuten, Polizisten oder Rettungssanitätern) ihre ministerialen Systeme zur Unterstützung der Krisenbewältigung (SWD) sind. Unter den Personen, die in Krisenmanagementstrukturen (auf Gemeinde- und Kreisebene) tätig sind, ist die Lösung aus Großpolen – „Arcus 2015.NET" – am bekanntesten. Es handelt sich dabei nicht um ein typisches Führungsunterstützungssystem, sondern eher um eine spezialisierte Datenbank über Kräfte und Mittel, die bei Kriseneinsätzen eingesetzt werden können, wodurch sie bei der Entscheidungsfindung im Krisenfall hilft.

Da es kein gemeinsames grenzüberschreitendes IT-System zur Unterstützung des Krisenmanagements gibt, könnten diese Funktionen möglicherweise durch IT-Komponenten auf Basis künstlicher Intelligenz (KI) übernommen werden, die einen angemessenen Informationsaustausch und damit die Zusammenarbeit zwischen den Krisenstrukturen der beiden Partnerstädte gewährleisten würden.

Künstliche Intelligenz ist eine neue Technologie, die jedoch vielen Anwendern bereits bekannt ist, denn 61 % der Befragten beantworteten Frage 5 der Umfrage positiv („Bitte geben Sie an, ob Sie in Ihrer Arbeit bereits mit Tools zu tun hatten, die künstliche Intelligenz nutzen? Kann sie Ihrer Meinung nach im Krisenmanagement eingesetzt werden?"). Die Antworten der Befragten deckten sich mit unseren Vermutungen: 68 % nannten Kommunikation, Informationsaustausch sowie Warnung und Alarmierung als die wichtigsten Merkmale von IT-Tools zur Unterstützung des Krisenmanagements. Das bedeutet, dass der Einsatz künstlicher Intelligenz zur Erfüllung dieser Funktionen die Effizienz der Zusammenarbeit zwischen deutschen und polnischen Strukturen steigern kann.

Zusammenfassend lässt sich sagen, dass es sich lohnt, die Zusammenarbeit zwischen den Krisenmanagementstrukturen auf deutscher und polnischer Seite auszubauen. Die Unterschiede in den Strukturen auf beiden Seiten verschwimmen, wenn es darum geht, konkrete Gefahren zu bekämpfen oder ihnen vorzubeugen. Wichtig sind dabei die zuvor getroffenen Vereinbarungen der Parteien hinsichtlich verschiedener Krisensituationen und Informationskanäle. In dieser Hinsicht lohnt es sich, KI-Tools zu nutzen, die dabei helfen können, insbesondere im Bereich der Online-Übersetzung. Eine gut etablierte Zusammenarbeit zeigt bereits hervorragende Ergebnisse, aber alle Änderungen (gesetzgeberischer Art auf polnischer Seite) führen zu Unsicherheiten hinsichtlich des Verhaltens des Partners, insbesondere aus einem anderen Land. Deshalb ist es so wichtig, bei Veränderungen, insbesondere bei Gesetzesänderungen, für einen gegenseitigen Informationsaustausch zu sorgen und die gegenseitigen Kompetenzen im Bereich der Sicherheit der Bewohner beider Seiten der Oder zu entwickeln.

Mikołaj TOMASZYK

KAPITEL VIII. DETAILLIERTE FORSCHUNGSERGEBNISSE

8.1. Forschungsmethodik

Das Projekt hat den Charakter eines Forschungs- und Schulungsprojekts und umfasst Empfehlungen für weitere Maßnahmen der Behörden im Grenzgebiet. Das Hauptziel des Projekts war:

- Ermittlung des Wissensstands der Projektteilnehmer über KI-Tools,
- Diagnose des Vertrauens der Projektteilnehmer in KI-Tools,
- Ermittlung möglicher Anwendungsbereiche für KI-Tools in der laufenden Zusammenarbeit von Behörden, Inspektionen, Grenzschutz und öffentlicher Verwaltung im Grenzgebiet.

Vor Beginn der Untersuchungen wurde eine Bibliotheksrecherche durchgeführt und Treffen mit Experten organisiert, um die Anwendungsbereiche von KI-Tools zu bestimmen und den Markt im Bereich der Führungsunterstützungssysteme in den polnischen Streitkräften zu erkunden. Anlässlich der Teilnahme als Experte an den Defence Days, die vom Think-Tank Defence.24 organisiert wurden, wurde das aktuelle Angebot von IT-Unternehmen, die KI-Anwendungen zur Koordinierung der Aktivitäten der Dienste anbieten, gesammelt und anschließend analysiert. Dank dieser Maßnahmen konnten Bereiche und Fragenkataloge festgelegt werden. Auf dieser Grundlage wurde mittels negativer Verifizierung ein Fragebogen erstellt, der in das Tool ankietaplus.pl/ aufgenommen wurde.

Es wurden zwei Versionen des Fragebogens erstellt: eine polnische und eine deutsche. Der Fragebogen bestand aus 23 inhaltlichen Fragen, die nach Themenbereichen geordnet waren. Die Fragen waren unterschiedlich aufgebaut – von einfachen Fragen, auf die eine präzise Antwort (Ja oder Nein) erwartet wurde, bis hin zu komplexen Fragen, bei denen die Befragten ihr Fachwissen im Zusammenhang mit ihrer Arbeit und ihre Meinung zu KI-Tools mitteilen mussten oder bei denen überprüft wurde, inwieweit die Befragten und ihre Arbeitgeber auf die Einführung von KI-Tools in der Kommunikation vorbereitet und bereit sind. Zu diesem Zweck wurde eine Lickert-Skala verwendet.

Die Fragen zum Wissen und zu den Meinungen über KI enthielten hingegen eine Reihe von Ansichten zu diesem Thema, die aus der Fachliteratur und einer Übersicht über den Markt für KI-Produkte stammen, wobei auch das Wissen von Experten genutzt wurde, die gleichzeitig als Trainer im Projekt tätig waren. Die Ergebnisse von Untersuchungen anderer Forscherteams oder von Sozialstudien, die in Branchenkreisen durchgeführt wurden, hatten Einfluss auf den Inhalt der Fragen und die Antwortmöglichkeiten. So geht beispielsweise aus den in der Tageszeitung „Rzeczpospolita" beschriebenen Untersuchungen der HRK hervor, dass:

- 86 % der Befragten davon überzeugt sind, dass KI die Personalverwaltung unterstützen wird und

- nur 7 % der Befragten gegenteiliger Meinung sind[88].

Die HR-Abteilungen, in denen laut den Befragten KI in den letzten zwei Jahren am dynamischsten eingeführt wurde, sind unter anderem: elektronische Dokumentenarchive, Signaturplattformen, Chatbots und andere. Andere Studien zeigen, dass Polen einer der führenden Märkte für die Entwicklung und Implementierung von KI-Tools ist. Am häufigsten werden KI-Tools bei der täglichen Arbeit eingesetzt, z. B. zum Vorschlagen von Antworten auf E-Mails oder zum Suchen von Informationen. Wie aus einer Studie von Molly Sands vom TeamworkLab hervorgeht, sparen Nutzer, die KI auf diese Weise einsetzen, Zeit und verbessern die Qualität ihrer Arbeit. Weniger Menschen nutzen KI-Tools für strategische Aktivitäten. In einer anderen Studie zu diesem Thema wird auf einen für dieses Projekt wichtigen Aspekt hingewiesen. Krzysztof Mazur identifiziert mehrere Hindernisse für die reibungslose Einführung von KI im Management und rät, keine Angst davor zu haben, da nach mehreren Jahren der Einführung von LLM-Sprachmodellen „die tatsächliche Beschäftigung in vielen Sektoren, die als am stärksten von der Automatisierung bedroht gelten, stabil bleibt oder sogar zunimmt"[89]. Der Autor weist zu Recht darauf hin, dass Personalengpässe und der Mangel an Fachkräften, die nicht nur über Kenntnisse in den Bereichen Informatik und Programmierung verfügen, sondern auch über fundierte Kenntnisse der Branche und der Bereiche, in denen KI die Aktivitäten unterstützen soll, ein Hindernis für die Einführung von LLM darstellen[90].

Die Interviews wurden auf verschiedene Weise durchgeführt. Die Befragten konnten den QR-Code kopieren und ihre Antworten online geben oder die vorbereiteten Interviewformulare ausfüllen (beide Versionen sind identisch), die vor den Schulungen verteilt wurden. Die Gruppe nahm an drei Schulungen teil, wobei die Befragung vor der ersten Schulung durchgeführt wurde. Daher hatten die Schulungsleiter Kenntnis über die Einstellung der Befragten zu den Themen des Projekts. Dadurch war es möglich, im praktischen Teil der Schulungen auf das Wissen und die Meinungen der Befragten Bezug zu nehmen und dieses Wissen anhand spezifischer Fallbeispiele zu erweitern und zu vertiefen.

Die Forschungsstrategie des Projekts sah vor, dass nach Abschluss der Diagnose- und Schulungsphase eine zweite Forschungsphase folgt – direkte Interviews mit ausgewählten Projektteilnehmern. Die in diesem Teil der Studie gestellten Fragen wurden auf der Grundlage des Berichts aus dem ersten Teil der Studie und der Analyse der Aussagen der Projektteilnehmer vorbereitet. Die Auswahl der Befragten hing von ihrem Arbeitsplatz und ihren Aufgaben ab. Die Gesamtanalyse der erzielten Forschungsergebnisse ermöglichte es dem Team, Schlussfolgerungen und Empfehlungen für weitere Maßnahmen zu erarbeiten. Zum Abschluss des Forschungs- und Schulungsteils des Projekts fand eine Zusammenfassung statt, in deren Rahmen den Teilnehmern die Teilnahme an einer offenen Diskussion „around the table" angeboten wurde, bei der Experten die Erzählung zu den in den direkten Interviews angesprochenen Themen moderierten. Die Schlussfolgerungen aus diesem Teil wurden ausgearbeitet und sind integraler Bestandteil der Forschungsphase des Projekts.

Die Auswahl der Stichprobe erfolgte auf der Grundlage einer Analyse der Organisationsstrukturen der Dienste, Inspektionen und Wachdienste, deren Organisationseinheiten sich im Funktionsbereich von

88 A. Błaszczak, Sztuczna inteligencja zatrudni pracowników i przyzna im premie (Künstliche Intelligenz wird Mitarbeiter einstellen und ihnen Prämien gewähren), „Rzeczpospolita" z dnia 21.07.2025.

89 K. Mazur, Jeszcze nie musimy bać się AI (Wir müssen uns noch keine Sorgen um KI machen), „Rzeczpospolita. PlusMinus" z dnia 16-17.08.2025, s. 5.

90 Por. Ibidem, s. 5.

Słubice und Frankfurt (Oder) befinden. Als ordnendes Element wurden die gesetzlichen Aufgaben und Tätigkeitsbereiche berücksichtigt, die der polnischen und deutschen Verwaltungsgliederung des Staates zugeordnet sind. Dabei wurde berücksichtigt, dass jedes Land eine andere Form hat, was sich wiederum auf die Verwaltungsgliederung auswirkt. Dies hängt letztlich mit der organisatorischen Unterordnung der Einheiten und den Ebenen der Zusammenarbeit der Vertreter der öffentlichen Verwaltung zusammen. Daher wurden Vertreter des Woiwoden von Lubuskie, der Landesregierung Brandenburgs sowie der auf beiden Seiten der Grenze tätigen Dienste, Inspektionen und Wachdienste zur Teilnahme an dem Projekt eingeladen.

Insgesamt nahmen 26 Befragte aus Polen und Deutschland an der Umfrage teil. Auf polnischer Seite bestand die Gruppe der Befragten aus Vertretern des Stadtamtes in Słubice, des Landratsamtes in Słubice, des Woiwodschaftsamtes mit Sitz in Gorzów Wielkopolski, des Marschallamtes der Woiwodschaft Lubuskie, der Gemeinden des Landkreises Słubice und der Sanitätsinspektion in Słubice. Auf deutscher Seite bestand die Gruppe der Befragten aus Vertretern des Landes Brandenburg, der Rettungsdienste, der Stadtverwaltung Frankfurt (Oder), der örtlichen Polizei und der Feuerwehr. Es ist anzumerken, dass trotz der versandten Einladungen zur Teilnahme an dem Projekt sowohl auf polnischer als auch auf deutscher Seite keine Vertreter einiger Dienste, Inspektionen und Feuerwehren entsandt wurden, die nach Einschätzung der Projektentwickler einen Beitrag leisten könnten, der sich auf die Ergebnisse auswirken würde. Aus diesem Grund wurden einige Änderungen an der Forschungsstrategie vorgenommen, die darin bestanden, die Teilnehmer und Experten zur Teilnahme an einer auf den Forschungsergebnissen basierenden moderierten Podiumsdiskussion sowie an einem Rundtischgespräch einzuladen. Dank dieser Maßnahme konnten die Bedürfnisse genauer diagnostiziert und die endgültigen Schlussfolgerungen und Empfehlungen präzisiert werden.

8.2. Forschungsergebnisse

Die erste Frage lautete, welches Kommandounterstützungssystem den Befragten bekannt ist. Von den sieben vorhandenen Systemen sollten drei angegeben werden. In der Reihenfolge wurden folgende Systeme genannt:

- Kommandounterstützungssystem der Staatlichen Feuerwehr – 50 %,
- Arcus 2015. NET – 38,9 %,
- Kommandounterstützungssystem der Polizei 33,3 % und ebenso viele Nennungen entfielen auf das System des staatlichen Rettungsdienstes.

Es ist hervorzuheben, dass die Effektivität der Antworten auf diese Frage bei 72 % lag, was damit zusammenhängt, dass ein Teil der Befragten ihre Aufgaben in anderen Positionen ausübt, die indirekt mit der Führung und Kommunikation in Krisensituationen verbunden sind. Die deutschen Befragten, die diese Frage beantworteten, gaben an, dass sie mit keinem dieser Systeme arbeiten, was jedoch nicht bedeutet, dass solche Systeme nicht zur Ausstattung der Dienste gehören. Vielmehr hängt dies damit zusammen, dass Personen aus der deutschen öffentlichen Verwaltung für das Projekt gemeldet wurden: die Stadt Frankfurt (Oder) und das Land Brandenburg. Im Verlauf der drei persönlichen Interviews wurde diese Frage erneut gestellt. Die erhaltenen Antworten zeigen, dass es auf deutscher Seite erstens Unterschiede in der Organisation der Dienste und der Aufteilung ihrer Zuständigkeiten gibt, was einen

direkten Vergleich mit den derzeit in Polen eingesetzten Systemen zur Unterstützung der Kommunikation in Krisensituationen nicht zulässt. Zweitens werden die Maßnahmen der Dienste während der Arbeitszeiten der deutschen Verwaltung vom Kooperationszentrum unterstützt, das die Beamten bei zweisprachigen Kontakten unterstützt. Mit der Schließung dieses Büros beschränkt sich die Kommunikation jedoch auf die offizielle Kommunikation, die aufgrund der Unterschiede in der Organisation auf polnischer Seite die Einbeziehung des Koordinationszentrums mit Sitz in Gorzów Wielkopolski erforderlich macht. Ein solcher Kommunikationsfluss verlängert die Reaktionszeit. Um eine schnelle Kommunikation zu gewährleisten, werden daher polnischsprachige Personen eingesetzt, die teilweise die polnische Staatsbürgerschaft besitzen und auf der westlichen Seite der Grenze arbeiten.

In der nächsten Umfragefrage wurden die Befragten gebeten, anzugeben, mit welchem System sie konkret arbeiten. Den Befragten standen mehrere Antwortmöglichkeiten zur Verfügung, darunter ein Feld für eigene Antworten. Aus den möglichen Antworten wurden folgende ausgewählt: ARCUS Car, Zentrale Meldeapplikation und SWD der Polizei. Die deutsche Seite weist in direkten Interviews darauf hin, dass jeder Dienst mit seinem eigenen System arbeitet und nicht offen für eine Änderung ist. Dies kann bedeuten, dass diese Systeme zuverlässig, optimal und handlich sind. Gleichzeitig wurde auf die Notwendigkeit hingewiesen, eine Schnittstelle für diese Systeme zu entwickeln, mit der die Daten aller Dienste miteinander verknüpft werden könnten: Aufgabendokumentation, Meldungen und Informationsübermittlung. In diesem Zusammenhang betonte einer der Befragten im direkten Interview, dass angesichts der beiden Seiten bekannten Hindernisse für die grenzüberschreitende Zusammenarbeit und der Inkompatibilität der Kommunikations- und Krisenmanagementsysteme Unterstützung für Maßnahmen in den Grenzgebieten der Mitgliedstaaten der Europäischen Union durch deren Institutionen zu erwarten sei. Diese Maßnahmen sollten ein Ziel verfolgen: die Annäherung des zivilen Sektors, der Dienste, Inspektionen und Wachdienste sowie des militärischen Sektors[91].

Anschließend wurden die Befragten gebeten, die Frage zu beantworten, mit welchen grenzüberschreitenden Ereignissen sie in ihrer beruflichen Tätigkeit konfrontiert sind. Von den 11 möglichen Ereignissen sollten 5 ausgewählt werden. Darunter befanden sich folgende:

- Naturkatastrophen mit grenzüberschreitenden Auswirkungen (z. B. Waldbrände, Überschwemmungen),
- Verbreitung von Desinformation und Propaganda durch soziale Medien,
- Ausbreitung von Infektionskrankheiten (z. B. COVID-19, Vogelgrippe, SARS, Tuberkulose),
- Luft- und Wasserverschmutzung (z. B. Smog, Chemikalienaustritt in Flüsse, die durch mehrere Länder fließen),
- Massenmigration aufgrund von Krieg, Armut, Klimawandel.

Auf deutscher Seite wurden ähnliche Ereignisse genannt, darunter in erster Linie Naturkatastrophen: Luftverschmutzung, chemische Verschmutzung von Flüssen, Krisenereignisse mit grenzüberschreitenden Auswirkungen wie Brände, Hackerangriffe auf kritische Infrastrukturen und internationale Kriminalität. Es wurde auch darauf hingewiesen, dass die Nähe zur Autobahn eine Quelle

[91] Maßnahmen in diesem Bereich wurden während der polnischen EU-Ratspräsidentschaft im Rahmen der Cyber Commandes im ersten Halbjahr 2025 erörtert.

für Krisensituationen in beiden Städten ist. Es wurde auf Verkehrsstaus hingewiesen, die dazu führen, dass der Kfz-Verkehr über den Grenzübergang FF/O – Słubice geleitet wird, was zu Staus in der Stadt führt und beispielsweise den Einsatzkräften den Weg zu ihren Einsatzorten erschwert. Während der abschließenden Diskussion über das Projekt äußerten sich die Teilnehmer des Rundtischgesprächs anerkennend darüber, dass dank der Zusammenarbeit der Dienste auf beiden Seiten der Grenze die mit der Einführung der Grenzkontrollen verbundenen Staus kein Problem mehr für das normale Funktionieren beider Städte und ihrer Einwohner darstellen.

Ein hohes Verkehrsaufkommen geht mit einer höheren Wahrscheinlichkeit von Verkehrsunfällen einher, die eine schnelle Reaktion erfordern und die Einweisung der Verletzten ins Krankenhaus notwendig machen können. Der Zugang zu medizinischer Versorgung in Krankenhäusern ist auch in Fällen von Bedeutung, in denen polnische Staatsbürger, die in Deutschland arbeiten, die deutsche Krankenversicherung in Anspruch nehmen. Diese berechtigt sie zur Inanspruchnahme medizinischer Versorgung im deutschen Gesundheitswesen. Die Versorgung dieser Patienten durch medizinische Einrichtungen auf beiden Seiten der Grenze ist eine weitere Herausforderung für die Zusammenarbeit. Meistens erfolgt dies über inoffizielle Kanäle, da in Situationen, die die Gesundheit und das Leben der Patienten gefährden, schnelles Handeln erforderlich ist.

In der grenzüberschreitenden Zusammenarbeit ist ein häufiger Grund für deren unbefriedigende Qualität weniger der Mangel an Bereitschaft und Willen zur Zusammenarbeit, sondern vielmehr Hindernisse und Barrieren unterschiedlicher Art. Diese müssen identifiziert werden, bevor Maßnahmen zur Einführung von KI-Tools in die laufende Arbeit der Verwaltung und der Behörden ergriffen werden. Auf diese Weise wird das Risiko verringert, dass ein Tool eingeführt wird, das die Arbeit nicht unterstützt, sondern zusätzlich erschwert und ein weiteres Hindernis für die Zusammenarbeit darstellt. Um diese zu identifizieren, wurde daher folgende Frage gestellt: „Bitte geben Sie auf der Grundlage Ihrer Berufserfahrung an, welche Faktoren, Ereignisse und Praktiken die Erfüllung Ihrer beruflichen Pflichten und Aufgaben am meisten behindern. Bitte wählen Sie maximal 5 Hindernisse aus.“ Die Befragten nannten folgende Hindernisse:

- Fehlen gemeinsamer Pläne und Verfahren für Krisensituationen und grenzüberschreitende Notfälle,
- nicht an die grenzüberschreitenden Gegebenheiten angepasste Struktur der Zuständigkeitsverteilung zwischen Behörden und Verwaltungen,
- Schwierigkeiten bei der operativen Kommunikation (Fehlen einer gemeinsamen Arbeitssprache),
- fehlende Interoperabilität der IT-Systeme (fehlende gemeinsame Datenbanken),
- unterschiedliche nationale und politische Interessen.

Die deutschen Befragten hingegen nannten in erster Linie Probleme beim Datenaustausch zwischen den Parteien in Echtzeit. An zweiter Stelle folgten die unterschiedliche Aufteilung der Zuständigkeiten zwischen Verwaltung und Dienststellen auf beiden Seiten der Grenze sowie deren unterschiedliche

Struktur, nämlich hierarchisch auf polnischer und horizontal auf deutscher Seite. Darüber hinaus wurde auf das Fehlen gemeinsamer Aktionspläne für Krisensituationen, das Fehlen gemeinsamer Übungen, unterschiedliche Organisationskulturen, Führungsstile sowie Ausbildungssysteme für Dienste und Verwaltung hingewiesen.

Die Analyse dieser Antworten zeigt, dass nach wie vor die Staatsgrenze, aber auch Unterschiede im System der Aufgaben- und Zuständigkeitsverteilung im Bereich der Sicherheit der Einwohner das größte Hindernis für die derzeitige Zusammenarbeit der Verwaltungen und Dienste darstellen. Darüber hinaus empfinden beide Gemeinschaften trotz ihrer Nachbarschaft die mangelnde Kenntnis der Sprache des Nachbarn als Hindernis. In solchen Situationen wird meist eine gemeinsame Sprache gewählt, in der beide Seiten kommunizieren können. In der Regel ist diese sogenannte dritte Sprache Englisch. In direkten Interviews wurde jedoch festgestellt, dass die Mitarbeiter der Dienste und Verwaltungen auf beiden Seiten der Grenze keine zufriedenstellenden Kenntnisse dieser Sprache aufweisen.

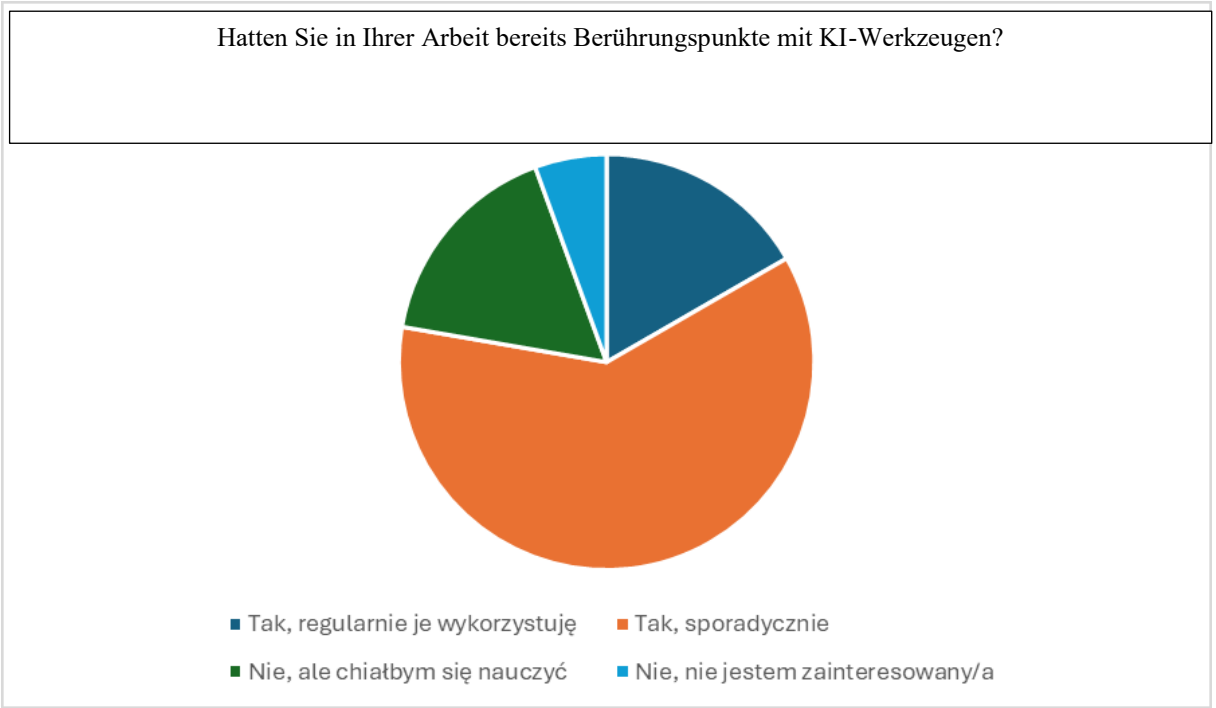
Beachtenswert sind die Antworten der deutschen Befragten, die den geringen Grad der Zusammenarbeit zwischen den Behörden in der Region Słubice und Frankfurt auf Hindernisse zurückführen, die nach Ansicht der Autoren dieser Studie relativ leicht zu überwinden sind. Es scheint, dass durch eine gemeinsam ausgearbeitete Vereinbarung Raum für Zusammenarbeit in folgenden Bereichen geschaffen werden kann: gemeinsame Übungen, Informationsaustausch, Koordinierung von Krisenmanagementplänen. Die empfohlene Methode für eine solche Zusammenarbeit ist die offene Koordinierungsmethode, die aus den Erfahrungen der Zusammenarbeit der Staaten in der Europäischen Union bekannt ist.

In den direkten Interviews wurde auch eine Frage zu dem in Słubice ausgearbeiteten und am 18. Juli 2002 unterzeichneten Abkommen zwischen dem Minister für Inneres und Verwaltung der Republik Polen und dem Ministerium des Innern des Landes Brandenburg über gegenseitige Hilfe bei Katastrophen, Naturkatastrophen und anderen schweren Unfällen[92]. Bis zum Zeitpunkt der Durchführung der Untersuchungen wurde diese Vereinbarung nicht aktualisiert. Einer der Befragten äußerte in einem persönlichen Interview die Meinung, dass der Inhalt des Dokuments nicht in dem Maße genutzt werde, wie es eigentlich vorgesehen sei. Es wurde auf die Möglichkeit hingewiesen, auf der Grundlage seines Inhalts und der erforderlichen Organisation von Arbeitstreffen beider Seiten, deren Gegenstand sich auf den Informationsaustausch, die Synchronisierung von Krisenreaktionsplänen, die Identifizierung von Kommunikationsblockaden und die Bewertung von Maßnahmen beziehen sollte. Ein wichtiger Aspekt solcher Treffen ist, vorausgesetzt, dass die Gruppe der Teilnehmer nicht wechselt, der Aufbau von Beziehungskapital, das die Kommunikation verbessert und Vertrauen schafft. Es ist zu erwarten, dass mit dem Inkrafttreten neuer Rechtsvorschriften über den Zivilschutz und den Katastrophenschutz in Polen der Inhalt dieses Dokuments einer Bewertung unterzogen und an die neuen Gegebenheiten angepasst wird. Die zweite Erwartung betrifft die Änderung des pauschalen Charakters dieser Vorschriften und ihre Umsetzung in konkrete Maßnahmen und Formen der Zusammenarbeit.

92 Źródło: Porozumienie między Ministrem Spraw Wewnętrznych i Administracji Rzeczypospolitej Polskiej a Ministerstwem Spraw Wewnętrznych Brandenburgii o wzajemnej pomocy podczas katastrof, klęsk żywiołowych i innych poważnych wypadków, sporządzone w Słubicach dnia 18 lipca 2002 r., M.P. 2003 nr 15 poz. 211, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20030150211/O/M20030211.pdf (dostęp: 06.10.2025).

Der nächste Fragenblock betraf die Erfahrungen der Befragten mit KI-Tools und ihre Bereitschaft, diese in ihrer Arbeit einzusetzen. Die Antworten sind in der folgenden Grafik 1 dargestellt.

Abbildung 3: Nutzung von KI-Tools am Arbeitsplatz durch die Befragten



Tak, regularnie je wykorzystuję	→	Ja, ich nutze sie regelmäßig
Tak, sporadycznie	→	Ja, gelegentlich
Nie, ale chciałbym się nauczyć	→	Nein, aber ich würde es gerne lernen
Nie, nie jestem zainteresowany/a	→	Nein, ich bin daran nicht interessiert

Quelle: Eigene Untersuchung, n – 26.

Die Antworten der Befragten, die täglich in der deutschen Verwaltung arbeiten, unterschieden sich nicht von den Antworten ihrer Kollegen und Kolleginnen aus Polen.

Interessant sind die Ergebnisse, die nach der Frage nach den Überzeugungen der Befragten zum Einfluss von KI-Tools auf verschiedene Lebensbereiche, darunter auch das Berufsleben, gesammelt wurden. Die Teilnehmer der Umfrage sollten auf einer Skala von 1 bis 5, wobei 1 für „stimme überhaupt nicht zu" und 5 für „stimme voll und ganz zu" steht, zu verschiedenen Thesen im Zusammenhang mit KI Stellung nehmen. Aus den Antworten geht hervor:

- AI-Tools stellen nach Meinung der Befragten keine Gefahr für ihren Arbeitsplatz dar (52,9 % der Antworten mit einer Bewertung von 5 auf der Skala und 23,5 % mit einer Bewertung von 4). In einer zweiten, inhaltlich ähnlichen Frage wurden die oben genannten Überzeugungen der Befragten bestätigt, da 61,1 % von ihnen angaben, dass KI nicht in naher Zukunft alle Arbeitnehmer ersetzen werde, während nur 11,2 % der Befragten der gegenteiligen Meinung waren. In Bezug auf das Risiko, dass KI den Befragten an seinem Arbeitsplatz ersetzen könnte, wählte die überwiegende Mehrheit der Befragten die

Optionen 1 und 2 – insgesamt 76,5 %. Zwei Befragte, d. h. 11,8 % der Befragten, sind weder positiv noch negativ davon überzeugt. Etwas weniger optimistisch gegenüber KI sind die deutschsprachigen Befragten, deren Meinung über die Möglichkeit, durch künstliche Intelligenz am Arbeitsplatz ersetzt zu werden, etwas weniger eindeutig ist und die Angst vor dem Verdrängung aus dem Arbeitsmarkt zum Ausdruck bringen – 72 % der Antworten stimmen eher zu. Der Optimismus der Befragten wird durch die Meinungen der KI-Entwickler nicht bestätigt.Laut Dario Amodei könnte KI in den nächsten fünf Jahren sogenannte White-Collar-Jobs ersetzen, d. h. Tätigkeiten auf der untersten Ebene, bei denen es um geistige, Büro- oder Verwaltungsarbeit geht.[93]. Dieser Prozess kann länger dauern, da die Unternehmensleitungen sich gegen die Einführung von KI sträuben, wie auch Untersuchungen zeigen[94]. Man kann sich eine Situation vorstellen, in der ähnliche Befürchtungen die Haltung der Führungskräfte in öffentlichen Verwaltungsbehörden prägen werden.

- Die überwiegende Mehrheit der Befragten lehnte die Ansicht ab, dass KI bessere Entscheidungen trifft als Menschen – insgesamt gaben 88,3 % der Befragten die Antworten 1 und 2 auf der Skala an. Eine andere Meinung vertrat eine Gruppe von Befragten aus Deutschland, die keine so gefestigte Meinung darüber haben, ob KI bessere Entscheidungen trifft als Menschen. Die Befragten auf beiden Seiten der Grenze wurden zu ihrer Meinung zu diesem Thema befragt, da „mit dem Aufkommen der generativen KI die Technologie nicht nur Inhalte generiert, sondern auch Entscheidungen treffen und konkrete Maßnahmen ergreifen kann”[95].

- 66,6 % der polnischen Befragten sind davon überzeugt, dass KI keine Gefahr für die gesamte Menschheit darstellt. Es ist anzumerken, dass 11,1 % der Befragten der gegenteiligen Meinung sind und eine solche Gefahr bejahen, während 22,2 % dieser Aussage weder zustimmen noch widersprechen. Die deutschsprachigen Befragten nahmen zu dieser Frage eine eher zurückhaltende Haltung ein. 50 % von ihnen haben keine Meinung zu diesem Thema, während 25 % der Meinung sind, dass KI eine Gefahr für die Menschheit darstellt. Die Analyse der Antworten auf diese Frage gibt einen klaren Einblick in das potenzielle Vertrauen in KI und die Wahrnehmung ihrer Rolle und Möglichkeiten zur Unterstützung im täglichen und beruflichen Leben.

- 83,2 % der polnischen Befragten sind der Meinung, dass KI-Tools ihnen bei der Erfüllung ihrer beruflichen Aufgaben helfen können. Diese Überzeugung entspricht der Erwartung, dass KI-Tools die Produktivität der Mitarbeiter steigern werden. Diese Aussage treffen 72,1 % der Befragten aus Polen (Noten 4 und 5) und 75 % aus Deutschland. Gleichzeitig zeigen die Antworten der Befragten auf die Aussage, dass KI-Tools sie bei ihrer täglichen Arbeit unterstützen, dass die Meinungen zu diesem Thema auseinandergehen. Die summierten

93 Za: A. Bartkiewicz, Kogo zwolni sztuczna inteligencja? Jedna kluczowa kompetencja pracownika przyszłości (Wen wird die künstliche Intelligenz entlassen? Eine Schlüsselkompetenz des Arbeitnehmers der Zukunft), „Rzeczpospolita. PlusMinus” z dnia 14-15.06.2025, s. 4.

94 Por. K. Mazur, Jeszcze nie musimy..., op. cit., s. 5.

95 Ibidem, s. 4.

Bewertungen 1 und 2 zeigen, dass 44,5 % der Befragten dieser Meinung nicht zustimmen, während die Option „stimme zu" und „stimme voll und ganz zu" insgesamt 33,3 % der Befragten Zustimmung fand. Dieses Ergebnis könnte darauf hindeuten, dass die an der Umfrage teilnehmenden Vertreter der Verwaltung und der Behörden offen für innovative Lösungen sind, die ihre Arbeit unterstützen, aber skeptisch gegenüber einer möglichen Unterstützung ihres Lebens durch KI sind.

- Nur 52,2 % der Befragten aus Polen geben an, dass sie wissen, wie KI-Tools funktionieren. Im Vergleich dazu geben 75 % der deutschsprachigen Befragten an, über Kenntnisse in diesem Bereich zu verfügen. 23,4 % der Befragten sind anderer Meinung, während 17,6 % der Befragten eine neutrale Antwort gewählt haben. Gleichzeitig geben insgesamt 94,5 % der Befragten aus Polen und 75 % aus Deutschland an, dass sie sich darüber informieren möchten, wie sie KI an ihrem Arbeitsplatz nutzen können. Die Befragten wissen, dass KI nicht nur aus Chatbots und Sprachassistenten besteht (66,6 % der Befragten), sondern auch, dass KI offen ist, d. h. sie interpretiert das, was wir ihr eingeben (55,6 % der Befragten). Darüber hinaus sind sie sich bewusst, dass KI Fehler macht (83,4 %) (100 % der zweiten Gruppe von Befragten) und zur Selbstverbesserung fähig ist – 66,6 % der Befürworter dieser Ansicht (75 % aus Deutschland) und 27,8 % der Befragten, die sich gegenüber dieser Meinung distanzieren. Die Gesamtinterpretation dieser Ergebnisse zeigt das Wissen und Bewusstsein der Vertreter der Verwaltung und der am Projekt beteiligten Dienste über KI und deren Auswirkungen auf das tägliche und berufliche Leben. Sie sind bereit, sich über Möglichkeiten zur Verbesserung ihrer Arbeit zu informieren, und bringen ihre Skepsis hinsichtlich der Zuverlässigkeit von KI-Tools und deren Eignung für die Gewährleistung der Sicherheit der Einwohner klar zum Ausdruck.

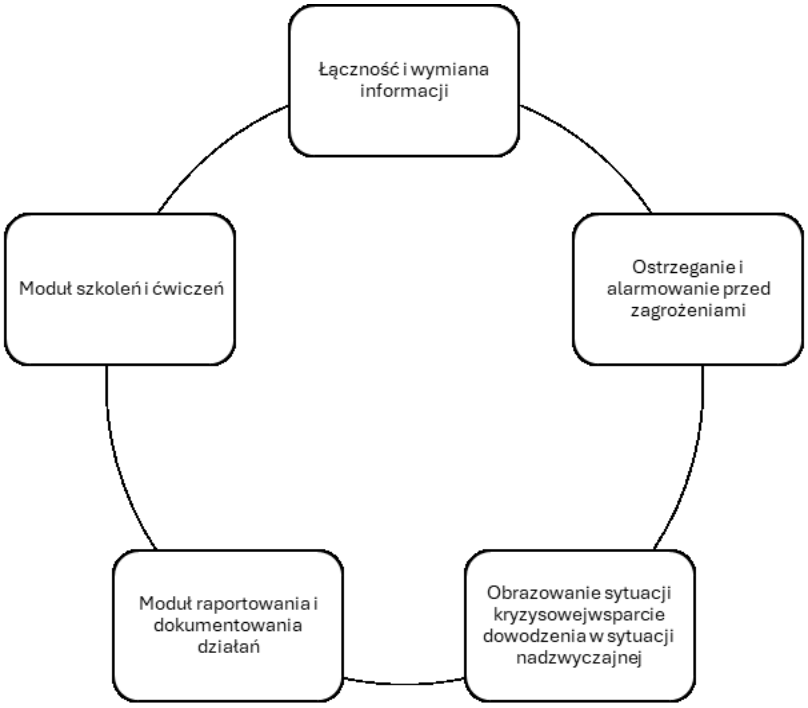
  Um zufriedenstellend zu funktionieren, benötigt KI qualitativ hochwertige Daten, die von gut ausgebildeten Menschen generiert werden. Wenn wir dies nicht gewährleisten, wird das System „dümmer" werden[96], es wird zu Informationschaos führen und Fehlinformationen verbreiten. Nur diejenigen, die über tatsächliches Wissen verfügen, werden dies erkennen und überprüfen können, während andere nicht über die Kompetenz für eine solche Überprüfung verfügen und möglicherweise falsche Informationen weiterverbreiten.

  Die Befragten haben keine eindeutige Meinung dazu, ob KI-Tools ihrer Meinung nach ein Mittel zur Gewährleistung der Sicherheit von Menschen sind. Die Ansicht, dass „eine Armee mit weniger Personal dank KI einen Krieg gewinnen kann", fand ebenso viele Befürworter wie Skeptiker, wobei 27,8 % der Befragten sich überhaupt nicht damit identifizieren können. Auf der Grundlage der gesammelten Antworten kann die Haltung der Befragten als skeptisch bewertet werden, wobei ein Interesse an der Nutzung dieser Instrumente zur Gewährleistung der Sicherheit der Bevölkerung besteht. Mehr Optimismus zeigten Vertreter der deutschen Grenzverwaltung – 75 % der Befragten waren der Meinung, dass KI zur Gewährleistung der Sicherheit der Bevölkerung beitragen kann. Hervorzuheben ist, dass 82,3 % der Befragten sich mit der Aussage identifizieren, dass sie sich für KI interessieren.

96 Por. K. Mazur, Jeszcze nie musimy..., op. cit., s. 6.

Neben der Frage zur Wahrnehmung von KI im Berufsleben wurden die Befragten auch zu ihren Erwartungen hinsichtlich der Funktionen eines Führungsunterstützungssystems befragt. Dabei wurde davon ausgegangen, dass das IT-System für sie benutzerfreundlich sein muss und dass seine Nutzer aufgrund ihrer Erfahrung in der Lage sind, seine potenziellen Funktionen zu bestimmen. Die gesammelten Antworten sind in Grafik 2 dargestellt.

Diagramm 1. Von den Befragten erwartete Funktionen des Führungsunterstützungssystems, die bei der Ausübung ihrer dienstlichen Aufgaben wünschenswert sind



Łączność i wymiana informacji → Kommunikation und Informationsaustausch
Ostrzeganie i alarmowanie przed zagrożeniami → Warnung und Alarmierung vor Gefahren
Moduł szkoleń i ćwiczeń → Modul für Schulungen und Übungen
Moduł raportowania i dokumentowania działań → Modul für Berichterstattung und Dokumentation von Maßnahmen
Obrazowanie sytuacji kryzysowej / wsparcie dowodzenia w sytuacji nadzwyczajnej → Lagebild-Darstellung / Führungsunterstützung in Notlagen

Quelle: Eigene Untersuchungen, n – 26.

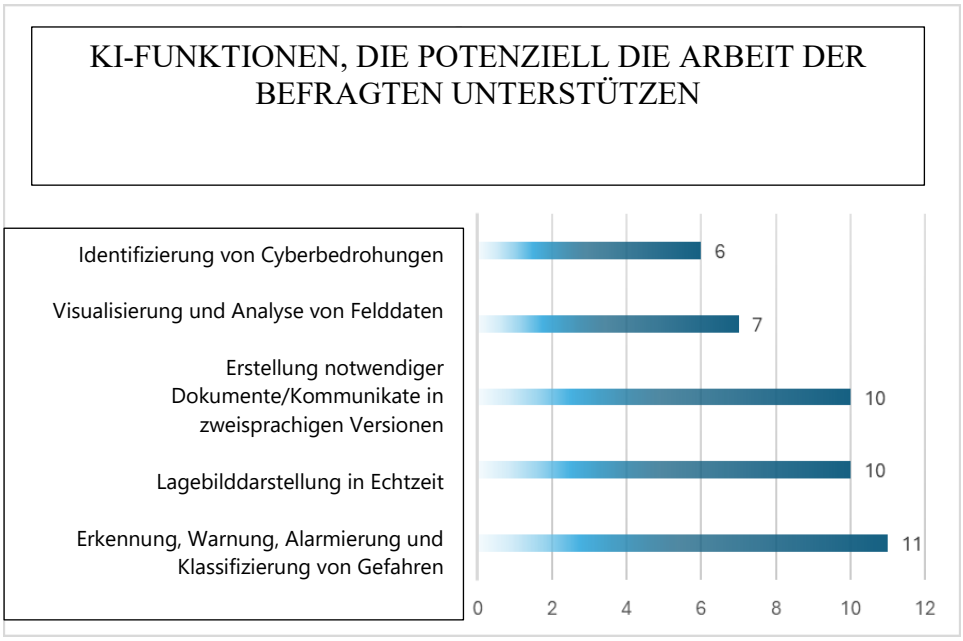
Die in Grafik 2 dargestellten Daten wurden erhoben, nachdem den Befragten die Frage gestellt wurde, welche Funktionen sie von einem beliebigen Führungsunterstützungssystem an ihrem Arbeitsplatz erwarten würden. Diese Erwartungen sind in der Meinung beider Gruppen von Befragten identisch, sie sind nichts Neues oder Innovatives, sondern entsprechen möglichen Krisensituationen, in denen eine effiziente Führung und schnelle Reaktion erwartet werden. Die Technik kann in diesem Bereich diejenigen unterstützen, in deren Händen die Sicherheit von Menschen und Eigentum liegt. Diese Ergebnisse sind in Verbindung mit den in Abbildung 3 dargestellten Ergebnissen zu interpretieren.

Die in Grafik 3 zusammengefassten Ergebnisse beziehen sich genau auf die Erwartungen der Mitarbeiter der Krisenmanagementabteilung auf beiden Seiten der Grenze an KI-Tools, die ihre Arbeit potenziell

unterstützen könnten. Es ist anzumerken, dass die Befragten diejenigen Funktionen genannt haben, die ihnen ihre Aufgaben nicht abnehmen, sondern sie potenziell dabei unterstützen sollen.

Dies sind vernünftige Erwartungen, die zum Zeitpunkt der Erstellung des Berichts mit der Technologie erfüllt werden können. Dazu gehören unter anderem die Unterstützung bei der Identifizierung von Cyber-Bedrohungen, die Visualisierung von Krisensituationen sowie die Erfassung und Analyse einer großen Anzahl von Daten und Variablen, die für Entscheidungen zum Schutz von Eigentum und Humanressourcen erforderlich sind. Derzeit werden auf dem Markt Kommandounterstützungssysteme angeboten, die Big Data-Analysen und Geländekartierung nutzen. Einige davon arbeiten mit Hilfe von KI. Von den dem Forschungsteam bekannten Systemen bietet keines die Möglichkeit, die Aktivitäten von Diensten aus verschiedenen Ländern, Menschen, die verschiedene Sprachen sprechen, und Systemen, die in zwei verschiedenen Rechtssystemen arbeiten, zu unterstützen.

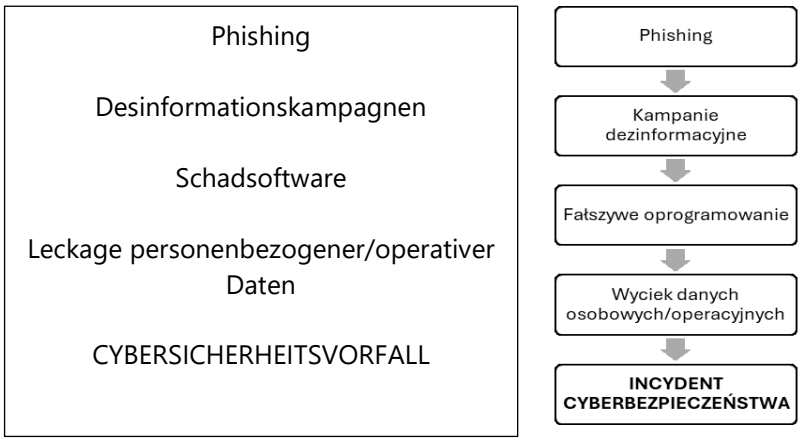
Diagramm 2. Erwartete KI-Funktionen, die am Arbeitsplatz der Befragten nützlich sind



Quelle: Eigene Untersuchungen, n – 26.

Mit einer weiteren Frage zur Identifizierung von Cybersicherheitsvorfällen sollte ermittelt werden, inwieweit sich die Befragten der möglichen Cyberbedrohungen nicht nur an ihrem Arbeitsplatz, sondern auch in ihrem Lebensumfeld bewusst sind. Diese Daten weichen nicht vom allgemeinen Wissensstand zu diesem Thema ab, was bedeutet, dass die Befragten auf beiden Seiten der Grenze sich dieser Gefahren bewusst sind und sie richtig benennen können.

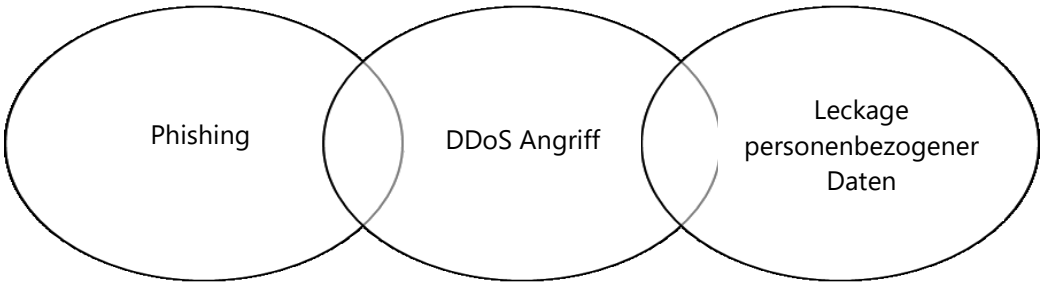
Abbildung 4. Arten von Cybersicherheitsvorfällen, von denen die Befragten in letzter Zeit gehört haben



Quelle: Eigene Untersuchung, N - 26.

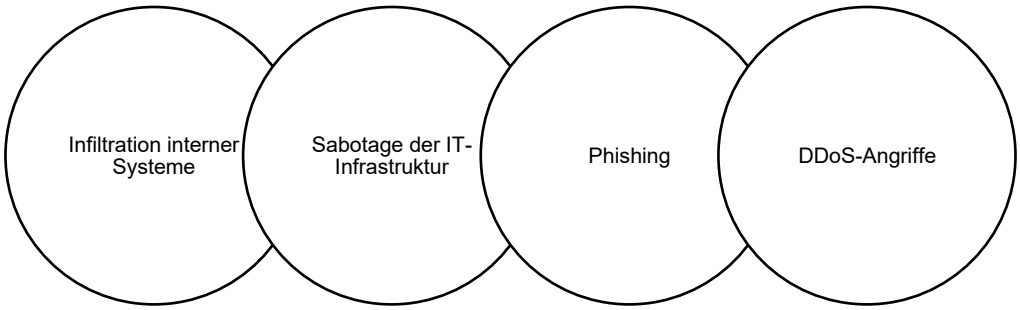
Aus Sicht der Arbeitsplätze, die die Befragten innehaben, wäre präziseres Wissen zu diesem Thema zu erwarten, das zusätzlich mit dem Umfang der ausgeführten Aufgaben identifiziert wird. Daher wurden die Befragten gebeten, Cybersicherheitsvorfälle an ihrem Arbeitsplatz zu identifizieren. Die Antwort auf diese Frage ist wichtig, um die Kommunikation zwischen den Diensten zweier verschiedener Länder mit Hilfe eines KI-Tools aufzunehmen und aufrechtzuerhalten. Man kann sich nämlich eine Situation vorstellen, in der eine an die Zivilbevölkerung gerichtete, von KI übersetzte Nachricht eine verschlüsselte Datei ist, die sensible Daten aus dem System einer anderen Behörde abzieht. Daher zeugen die drei möglichen (wenn auch unterschiedlichen) Vorfälle, die in den Abbildungen 5 und 5a dargestellt sind, vom Bewusstsein der Befragten, was sich möglicherweise in einer geringeren Anfälligkeit für deren Aktivierung niederschlägt.

Diagramm 3. Wahrgenommene Cybersicherheitsrisiken am Arbeitsplatz der Befragten aus Polen



Quelle: Eigene Untersuchungen, n – 18.

Diagramm 4. Wahrgenommene Cybersicherheitsrisiken am Arbeitsplatz der Befragten aus Deutschland



Quelle: Eigene Ausarbeitung, n – 8.

Wie im ersten Teil des Berichts erwähnt, wird in Studien zur Einführung von KI-Tools in den Entscheidungsprozess darauf hingewiesen, dass es notwendig ist, Regeln für die Nutzung von KI in Unternehmen oder Behörden zu entwickeln und umzusetzen sowie Kompetenzen für den sachgerechten Umgang mit diesen Tools zu vermitteln. Die Einführung einer behördlichen Richtlinie für die Nutzung von KI-Tools durch Mitarbeiter kann vor Datenlecks, Manipulationen mit Daten oder Reputationsverlusten schützen. Die Befragten wurden daher gefragt, ob in der Einrichtung, in der sie arbeiten, Verfahren zur Reaktion auf Cyberbedrohungen gelten. Die überwiegende Mehrheit der Befragten – 61,1 % – antwortete mit Ja, die Verfahren seien eingeführt und den Mitarbeitern bekannt. Nur 22,2 % der Befragten gaben an, dass es zwar Verfahren gibt, diese aber nicht allen Mitarbeitern bekannt sind. Die deutschsprachigen Befragten erteilten unterschiedlichere Antworten. Jede der möglichen Antwortoptionen wurde von einem gleichen Prozentsatz der Befragten ausgewählt – jeweils 20 % von ihnen.

Die Kenntnis der Verfahren ist wichtig, aber ebenso wichtig ist das Wissen der Studienteilnehmer über die grundlegenden nationalen und europäischen Rechtsvorschriften, die den Einsatz künstlicher Intelligenz im öffentlichen Sektor regeln. Nur 22,2 % der Befragten kennen die Grundsätze der EU-Verordnung zu KI – den sogenannten AI Act – sowie die polnischen oder deutschen Vorschriften zur Digitalisierung der Verwaltung. Etwas mehr als 60 % der Befragten geben an, über allgemeine Grundsätze für den Umgang mit personenbezogenen Daten zu verfügen. Ein anderes Bild der Kenntnis der EU- und nationalen Vorschriften zeigen die Befragten aus Deutschland. Drei Viertel der Befragten geben an, keine Kenntnisse über die EU- und nationalen Vorschriften zur KI zu haben. Nur ein Befragter gab an, diese Vorschriften zu kennen, aber keine detaillierten Kenntnisse darüber zu haben. Diese Daten bestätigen, dass ethische Richtlinien für KI im öffentlichen Sektor und darüber hinaus weiterhin kontinuierlich verbreitet werden müssen. Den Mitarbeitern der öffentlichen Dienste und Verwaltungen mangelt es an Kenntnissen über die wichtigsten Vorschriften in diesem Bereich. Diese Schlussfolgerung wird durch die Antworten der Umfrageteilnehmer auf die Frage nach ihrem Wissen über den grenzüberschreitenden Datenaustausch in Krisensituationen bestätigt. 38,9 % der Befragten geben an, dass sie die allgemeinen Grundsätze kennen, aber nicht die detaillierten Vorschriften, 27,8 % von ihnen

kennen diese Vorschriften nicht, und nur 11,1 % der Befragten geben an, dass sie diese Vorschriften gut kennen. Wenn die Mitarbeiter also nicht über ausreichende Kenntnisse in dem untersuchten Bereich verfügen, sollten sie daran interessiert sein, sich diese anzueignen. Aus diesem Grund wurde die Frage gestellt, welche Schulungen im Bereich KI und Krisenmanagement sie sich wünschen würden. Die erhaltenen Antworten zeigen, dass das Interesse der Befragten an diesem Thema groß ist und sich unter anderem auf folgende Bereiche bezieht:

- grenzüberschreitende Zusammenarbeit und Vereinbarkeit von Verfahren,
- den Schutz personenbezogener Daten und der Privatsphäre,
- Kommando- und Kontrollsysteme im Krisenmanagement,
- die Darstellung der Krisensituation in Echtzeit,
- die Überwachung und Analyse von Daten aus sozialen Medien sowie die Aufdeckung von Desinformation.

Die deutschen Befragten bekunden Interesse an Schulungen zu den Themen Erkennung, Überwachung und Alarmierung bei Gefahren mit Unterstützung von KI sowie an Schulungen zum Thema Schutz personenbezogener Daten und Schutz der Privatsphäre. Der dritte Bereich, der von ihnen am häufigsten genannt wird, ist der Einsatz von KI bei der Erstellung und Bewältigung von Krisensituationen in Echtzeit. Es ist anzumerken, dass trotz der zuvor gegebenen Antworten auf die Frage nach Schwierigkeiten und Hindernissen bei der grenzüberschreitenden Kommunikation keiner der Teilnehmer der polnischsprachigen Umfrage die Antwort „Übersetzung von Mitteilungen und Warnmeldungen ins Polnische und Deutsche" gewählt hat. In der deutschsprachigen Version der Umfrage wies ein Befragter auf die Notwendigkeit hin, KI bei der Übersetzung von Informationen und Meldungen aus dem Polnischen ins Deutsche und umgekehrt zu unterstützen. Zum Nachdenken regt auch die Tatsache an, dass nur ein einziger Hinweis auf Schulungen zur Erstellung der erforderlichen Dokumente/Mitteilungen in zwei Sprachen oder zur Automatisierung und Aggregation von Informationen über untergeordnete Einheiten zu finden ist. Es ist nämlich zu beachten, dass auf die Frage, ob sie bei ihrer Arbeit Übersetzungstools wie DeepL, Google Translate und andere verwenden, 55,6 % mit Ja antworteten und angaben, diese regelmäßig zu nutzen, während 38,9 % von ihnen angaben, diese nur gelegentlich zu verwenden (analog zu den deutschsprachigen Befragten). Insgesamt nutzen über 90 % der Befragten Online-Übersetzer (in Deutschland 100 %), was mit einem hohen Risiko einer fehlerhaften Übersetzung verbunden ist und somit die Anfälligkeit für die Weitergabe falsch übersetzter Informationen erhöht.

Im Anschluss an diese Frage wurden weitere Fragen zu den sprachlichen Schwierigkeiten gestellt, mit denen die Befragten im Zusammenhang mit der grenzüberschreitenden Zusammenarbeit konfrontiert sind. Die überwiegende Mehrheit der Befragten gab an, dass das Fehlen einer gemeinsamen Arbeitssprache ein Kommunikationsproblem darstellt, das das Verständnis der Fachterminologie erschwert. Das Fehlen einer Arbeitssprache ist nur für einen Befragten aus Deutschland ein Hindernis. Möglicherweise liegt der Grund dafür darin, dass die deutsche Verwaltung und die deutschen Behörden auch durch Personen mit polnischer Staatsangehörigkeit vertreten waren, die in Deutschland arbeiten. Darüber hinaus weisen die Befragten auf das Fehlen automatischer Systemübersetzungen hin, z. B. von Warnmeldungen und Dokumenten, die in Krisensituationen im Umlauf sind. Für die deutschen

Befragten ist dies das größte Hindernis für die Zusammenarbeit. Ein zweiter Umstand, der die grenzüberschreitende Zusammenarbeit erschwert, ist das Fehlen zweisprachiger Formulare und die fehlende Übersetzung der Krisenmanagementpläne des Nachbarn. Diese Mängel können dazu verleiten, allgemein zugängliche Tools zur Übersetzung von Inhalten zu verwenden. Dies ist jedoch, wie oben erwähnt, mit einem hohen Risiko verbunden. Gleichzeitig geben über 93 % der Befragten an, dass sie täglich oder mehrmals pro Woche verschiedene IT-Systeme bei ihrer Arbeit nutzen. ¾ der deutschen Partner, die an der Umfrage teilgenommen haben, nutzen täglich Online-Übersetzer.

Die polnischsprachigen Befragten, die diese Online-Übersetzer zumindest gelegentlich nutzen, geben gleichzeitig an, dass spezielle Übersetzungsprogramme für 61,1 % von ihnen sehr hilfreich und für 33,3 % hilfreich bei ihrer täglichen Arbeit im Kontakt mit ausländischen Partnern sein können. Für ihre Kollegen aus Deutschland sind diese Tools teilweise hilfreich. Es ist jedoch anzumerken, dass ihr Vertrauen in die Entscheidungen, die von KI-Systemen im Zusammenhang mit dem Krisenmanagement getroffen werden, einschließlich der Übersetzungen, gering ist. Nur 27,8 % der Befragten sind der Meinung, dass KI-gestützte Entscheidungen im Zusammenhang mit dem Krisenmanagement als vertrauenswürdig angesehen werden können (bei den deutschen Befragten verteilt sich das Vertrauen in KI gleichmäßig zwischen 2 und 4 auf einer Skala von 1 bis 5, wobei 1 für „kein Vertrauen" und 5 für „großes Vertrauen" steht. Die übrigen Befragten zeigen sich in dieser Frage skeptisch. Bei der Interpretation dieser Forschungsergebnisse fällt ein gewisser Widerspruch auf. Es ist lobenswert, dass Beamte und Mitarbeiter der Behörden bei der Nutzung von KI für ihre Arbeit Vorsicht walten lassen. Dieselben Mitarbeiter geben jedoch an, dass sie diese Geräte nutzen und darin ein Potenzial zur Verbesserung ihrer Arbeit sehen. Auf Nachfrage geben die deutschen Befragten an, dass trotz fehlender formaler Regelungen für den Einsatz von KI-Tools an ihrem Arbeitsplatz 75 % von ihnen diese Möglichkeiten nutzen. Dies ist ein wichtiger Faktor, der die Widerstandsfähigkeit des Krisenmanagementsystems verringert. Darüber hinaus erwarten sie von ihren Vorgesetzten, dass sie Regeln für den Einsatz von KI am Arbeitsplatz ausarbeiten, umsetzen und in der Praxis testen. Denn sie verfügen nicht über ausreichende Kenntnisse der nationalen und europäischen Vorschriften, die diese Fragen regeln.

Weitere Antworten der Befragten verdienen Beachtung. Sie wurden gebeten, ihre Einstellung zu Aussagen über die Nutzung von IT-Systemen in ihrer Arbeit auf einer Skala von 1 bis 5 zu bewerten, wobei 1 für „stimme überhaupt nicht zu" und 5 für „stimme voll und ganz zu" steht. Zusammenfassend lässt sich sagen, dass die Befragten auf beiden Seiten der deutsch-polnischen Grenze diese Systeme für ein effektives Krisenmanagement als entscheidend ansehen (94,4 %). 81,3 % der Befragten aus der polnischen Gruppe sind der Meinung, dass diese Systeme ihre Arbeit in Krisensituationen nicht behindern und dass sie in der Lage sind, sie zu nutzen (68,8 % positive Antworten). Die deutschsprachigen Befragten sind etwas anderer Meinung, da sie der Ansicht sind, dass die Führungsunterstützungssysteme ihre Arbeit teilweise behindern – insgesamt 75 % der Antworten auf 3 und 4 auf einer Skala von 1 bis 5. Die Befragten schätzen gleichzeitig das Vertrauen in ihre Kompetenzen, ihr Wissen und ihre Berufserfahrung, wobei der mit der Leitung von Maßnahmen verbundene Stress für beide Gruppen von Befragten kein wesentliches Hindernis für die Nutzung neuer Technologien darstellt. Diese Meinung wird durch die Antworten zur Nutzung von IT-Systemen in Krisensituationen und zur dafür erforderlichen Zeit bestätigt. Die Befragten beider Gruppen waren der Meinung, dass der Zeitmangel bei der Entscheidungsfindung in einer Notsituation für sie kein Hindernis darstellt. Sie würden jedoch erwarten, dass die Institution, in der sie arbeiten, die Entwicklung ihrer

digitalen Kompetenzen im Krisenmanagement unterstützt – durchschnittlich 43 % der Befragten sind mit dieser Haltung ihres Arbeitgebers zufrieden, während 57 % der Befragten auf die Notwendigkeit eines stärkeren Engagements ihres Arbeitgebers in diesem Bereich hinweisen.

Die Befragten der deutschsprachigen Gruppe sind mit der Unterstützung ihres Arbeitgebers bei der Entwicklung neuer Technologien im Bereich Krisenmanagement ausreichend zufrieden. Diese Antworten stimmen mit denen überein, die in Frage 15 zu der Häufigkeit von IT-Systemtests durch den Arbeitgeber, z. B. durch Penetrationstests, Audits usw., gegeben wurden. 38,9 % der Befragten geben an, dass diese Tests durchgeführt werden, jedoch unregelmäßig, während 38,9 % keine Kenntnisse darüber haben oder nicht wissen, ob dies der Fall ist (bei den deutschen Befragten hat die Hälfte keine Kenntnisse über die von ihren Arbeitgebern durchgeführten Cybersicherheitstests, während die andere Hälfte angibt, dass solche Tests regelmäßig, mindestens einmal im Jahr, durchgeführt werden. Daher sind die Vorsicht der Mitarbeiter und ihr begrenztes Vertrauen in solche Lösungen ein wertvoller Faktor für die Stärkung der Widerstandsfähigkeit des Entscheidungsprozesses im Krisenmanagement und der gegenseitigen Kommunikation in den untersuchten Einheiten. Zu den Faktoren, die die Widerstandsfähigkeit beeinträchtigen, gehören unter anderem fehlende Vorschriften am Arbeitsplatz und ein geringes Bewusstsein für die Notwendigkeit von Tests und Audits in diesem Bereich. Es besteht die Befürchtung, dass Mitarbeiter beispielsweise Online-Übersetzer nutzen und auf dieser Grundlage Entscheidungen treffen und Maßnahmen gegenüber Personen und Eigentum anordnen, ohne in der Lage zu sein, diese Inhalte zu überprüfen.

Es ist unmöglich, nicht auf ein weiteres Risiko hinzuweisen, das mit der Nutzung solcher Systeme durch Mitarbeiter in ihrer täglichen Arbeit verbunden ist. Aus den durchgeführten Untersuchungen geht nämlich hervor, dass nur 33,3 % der Projektteilnehmer in den letzten drei Jahren eine einmalige Schulung zu IT-Systemen im Management und in der Krisenkommunikation absolviert haben. Etwas mehr als 61 % (75 % in Deutschland) von ihnen haben keinerlei Schulung absolviert, und nur 22,2 % (in Deutschland – ein/e Befragte/r) planen, an einer solchen teilzunehmen. Gleichzeitig wird das Niveau der Cybersicherheit in den Einrichtungen, in denen die Befragten arbeiten, von 50 % der Befragten (Deutschland – 1 Befragter) als durchschnittlich und von 44 % von ihnen (Deutschland – 50 %) als sehr hoch eingeschätzt.

EMPFEHLUNGEN

Die effektive und sichere Implementierung von KI-Tools in der Kommunikation und im Krisenmanagement erfordert nicht nur die Auswahl der richtigen Technologie, sondern auch die Schaffung eines geeigneten organisatorischen und verfahrenstechnischen Ökosystems. Im Folgenden werden wichtige Empfehlungen vorgestellt, deren Umsetzung die Qualität der grenzüberschreitenden Zusammenarbeit erheblich verbessern und die Risiken im Zusammenhang mit Desinformation, Sprachbarrieren und Cyberbedrohungen verringern kann.

1. Die Ergebnisse der Umfrage zeigen, dass weiterhin die Staatsgrenze, aber auch Unterschiede im System der Aufgaben und Zuständigkeiten der Behörden im Bereich der Sicherheit der Einwohner das größte Hindernis für die derzeitige Zusammenarbeit zwischen Verwaltung und Behörden darstellen. Das Vorhandensein von Hindernissen in der Zusammenarbeit zwischen Behörden, Inspektionen und Wachdiensten sowie lokalen und staatlichen Verwaltungen im grenzüberschreitenden Bereich wirkt sich negativ auf die Sicherheit der in diesem Gebiet lebenden Bevölkerung aus. Darüber hinaus handelt es sich um Faktoren und Situationen, deren Auftreten die Widerstandsfähigkeit des Krisenmanagementsystems verringert. Eine Gesamtanalyse zeigt, dass diese sehr unterschiedlicher Natur sein können. Paradoxerweise werden mit dem technologischen Fortschritt einige Hindernisse, u. a. in Bezug auf die Übertragung, Sammlung von Informationen, Fernkommunikation, Echtzeit-Videoüberwachung und andere, beseitigt. Es entstehen jedoch neue Hindernisse, die ebenfalls beseitigt werden können, z. B. mit Hilfe von KI-Tools.

2. Die Identifizierung formaler Barrieren im Bewusstsein der Studienteilnehmer führt dazu, dass die aktuelle Zusammenarbeit auf informellem Wege auf der Grundlage des über Jahre hinweg aufgebauten Beziehungskapitals erfolgt. Einerseits sind solche Lösungen lobenswert, da sie effektiv sind. Langfristig wirken sie sich jedoch negativ auf die Effizienz und Zuverlässigkeit der Kommunikation und des Krisenmanagements aus. Mitarbeiter aller Dienste können bei der Arbeit fehlen, in den Ruhestand gehen oder den Arbeitsplatz wechseln. Ihr potenzielles Fehlen ist ein wesentlicher Risikofaktor und erhöht die Anfälligkeit des Systems für Instabilität. Daher sollte sich die Aufmerksamkeit aller Teilnehmer der Studie sowie ihrer Vorgesetzten auf die Entwicklung von Verfahren und dauerhaften Kommunikationskanälen konzentrieren. Die eingeführten Tools zur Übersetzung der Kommunikation im Krisenmanagement sollten auf Lösungen basieren, die keine KI verwenden, da diese einfacher und besser getestet sind und die mit der möglichen Verwendung von KI verbundenen rechtlichen Risiken ausschließen.

3. Das Fehlen einer effizienten, verständlichen Kommunikation zwischen den Mitarbeitern der Dienste auf beiden Seiten der polnisch-deutschen Grenze stellt einen wesentlichen Risikofaktor dar, der die Möglichkeit einer den Umständen angemessenen Reaktion auf eine Krisensituation dauerhaft beeinträchtigen kann. Natürlich können die Möglichkeiten, die KI im Krisenmanagement bietet, einen positiven Einfluss auf die Zusammenarbeit und Kommunikation der Dienste haben. Eine unsachgemäße Nutzung kann jedoch zu einer weiteren Krisensituation führen, die die negativen Auswirkungen noch verstärkt. In beiden Fällen ist der Mensch, sein Vertrauen und seine Bereitschaft, seine Arbeit mit KI-Tools zu unterstützen, ein Risikofaktor.

4. Die empfohlenen Maßnahmen weisen auf die Notwendigkeit hin, Technologien, Verfahren und menschliche Kompetenzen parallel weiterzuentwickeln. KI kann eine große Hilfe bei der mehrsprachigen Kommunikation und im Kampf gegen Desinformation sein, jedoch nur, wenn sie sicher und bewusst eingesetzt wird. Der Schlüssel liegt in der Synergie von Technologie, Sicherheit und Bildung – einer Kombination aus lokalen Modellen, Analysezentren, geschulten Betreibern und Audits.

5. Die in der öffentlichen Verwaltung tätigen Personen sind sich der Gefahren bewusst, doch selten wird dieses Bewusstsein in systematische Maßnahmen und objektive Tests der Widerstandsfähigkeit der Organisationen, in denen sie arbeiten, umgesetzt. Trotz des erklärten Willens, die Zusammenarbeit zu intensivieren und gemeinsame Übungen zu organisieren, bewerten die Befragten auf beiden Seiten der Grenze die bisherigen Erfahrungen damit als nicht zufriedenstellend. Gründe dafür sind unter anderem die mangelnde systematische Beteiligung am Projekt, die geringe Teilnahme von Entscheidungsträgern und Sprachbarrieren in beiden vertretenen Nationalitätengruppen. Es ist anzumerken, dass auf deutscher Seite in den Verwaltungsstrukturen der Dienste Personen beschäftigt sind, die fließend Polnisch und Deutsch sprechen. Im Laufe der Untersuchungen wurde festgestellt, dass dank dieser Personen Kommunikationsstörungen auf beiden Seiten minimiert werden können. Es ist jedoch zu beachten, dass diese Tatsache einer der wichtigsten Faktoren ist, die die Widerstandsfähigkeit der grenzüberschreitenden Zusammenarbeit beeinträchtigen. Ohne polnischsprachige Mitarbeiter auf deutscher Seite wird die Krisenkommunikation auf einem niedrigen Niveau bleiben, was sich negativ auf die Effizienz der Maßnahmen der Behörden auswirken wird.

6. Die Aufmerksamkeit des Forschungsteams wird auf Antworten der Befragten gelenkt, aus denen hervorgeht, dass nur 22,2 % der Befragten über Kenntnisse der Grundsätze der EU-Verordnung zu KI – dem sogenannten AI Act – sowie der polnischen oder deutschen Vorschriften zur Digitalisierung der Verwaltung verfügen. Etwas mehr als 60 % der Befragten geben an, über allgemeine Grundsätze für den Umgang mit personenbezogenen Daten Bescheid zu wissen. Ein anderes Bild hinsichtlich der Kenntnis der EU- und nationalen Vorschriften vermitteln die Befragten aus Deutschland. Drei Viertel der Befragten geben an, keine Kenntnisse über die EU- und nationalen Vorschriften zur KI zu haben. Nur ein(e) Befragte(r) gab an, diese Vorschriften zu kennen, aber keine detaillierten Kenntnisse darüber zu haben. Diese Daten bestätigen, dass im Bereich der Aufklärung über die Grundsätze der Nutzung von KI im öffentlichen Sektor und darüber hinaus weiterhin das Wissen über gesetzliche Vorschriften und Richtlinien im Bereich der KI-Ethik verbreitet werden muss.

7. Eine der Schlussfolgerungen aus den Untersuchungen, die Gegenstand dieser Studie sind, ist die Notwendigkeit, ein Krisenmanagementsystem zu entwickeln und zu implementieren, das alle Elemente des Systems integriert und IT-Tools nutzt. Die Verwendung von KI-Tools für diesen Zweck sollte mit Vorsicht betrachtet werden. Diese Skepsis ist durch die Haltung der Begünstigten gegenüber solchen Tools bedingt. Darüber hinaus ist darauf hinzuweisen, dass sich solche Tools noch in einer frühen Entwicklungsphase befinden und die rechtliche Bewertung ihrer Funktionsweise noch im Entstehen begriffen ist. Dies kann jedoch die potenzielle Möglichkeit des Einsatzes von KI in diesem Bereich nicht ausschließen.

8. Die Ergebnisse der Studie zeigen, dass die Rolle der KI in der mehrsprachigen Kommunikation zunimmt – bereits heute nutzen mehr als drei Viertel der Befragten solche Lösungen regelmäßig oder gelegentlich. Dies geschieht jedoch informell, ohne die notwendigen Regelungen innerhalb der Organisationen, in denen sie arbeiten. Die Befragten weisen deutlich auf die Notwendigkeit hin, dass KI-Tools Mitteilungen redigieren und in die Sprache des Nachbarn übersetzen. Der Einsatz von Tools wie PLLuM, Ollama, ChatGPT oder ElevenLabs kann nicht nur die Reaktionszeit verkürzen, sondern auch das Risiko von Fehlern aufgrund von Sprachbarrieren minimieren. In den kommenden Jahren ist zu erwarten, dass KI zu einem integralen Bestandteil grenzüberschreitender Krisenmanagementstrukturen wird, ähnlich wie heute digitale Funksysteme oder gemeinsame Datenaustauschplattformen zum Standard gehören. Die Qualität der übersetzten Texte ist wichtig. Eine fehlerhafte Übersetzung kann zu einer Krisensituation für die Einsatzkräfte, aber auch für die Zivilbevölkerung führen. Die Schlussfolgerungen aus den Untersuchungen, die auch direkte Interviews und eine rechtliche Analyse der bilateralen Vereinbarungen berücksichtigen, veranlassen uns jedoch zu der Feststellung, dass, bevor sich die polnische und die deutsche Seite für die Entwicklung eines eigenen Systems zur Unterstützung der Führung im grenzüberschreitenden Bereich entscheiden, die bestehenden rechtlichen Rahmenbedingungen und Instrumente zur Koordinierung der laufenden Zusammenarbeit genutzt werden sollten. Es wird daher empfohlen, regelmäßige Treffen zwischen Vertretern beider Seiten abzuhalten, um Informationen auszutauschen, Hindernisse für die Zusammenarbeit zu identifizieren, Kontakte zu verbessern und Risiken für die Stadt Frankfurt (Oder) und die Gemeinde Słubice zu ermitteln. Ein Teil der Befragten wies auf Gefahren hin, die auf beiden Seiten der Grenze bestehen, jedoch in einem Gebiet, das größer ist als das Gebiet, das von der Verwaltung der Stadt Frankfurt (Oder) und ihren Dienststellen sowie der Gemeinde Słubice und dem Landkreis Słubice abgedeckt wird. Daher sollte man sich in erster Linie auf das Krisenmanagement und die Krisenkommunikation der Dienste nur dieser beiden Städte und ihrer Funktionsbereiche konzentrieren. Die auf dieser Ebene entwickelten bewährten Verfahren können auf die Ebene der Woiwodschaft und des Bundeslandes übertragen werden.

9. Angesichts der Anfangsphase der Entwicklung der Technologie der künstlichen Intelligenz, zahlreiche und schwer zu beseitigende rechtliche Zweifel sowie Risiken aufgrund von Unterschieden in den Rechtssystemen und Strukturen des Krisenmanagements in Polen und Deutschland scheint eine Strategie der schrittweisen und vorsichtigen Einführung von KI-Lösungen in der grenzüberschreitenden Krisenkommunikation optimal zu sein. Die natürliche und rechtlich begründete Zurückhaltung der Beamten, Entscheidungen mit übermäßigem Risiko zu treffen, spricht dafür, mit Pilotprojekten in begrenztem Umfang zu beginnen. Im Rahmen solcher Projekte ist es möglich, die identifizierten Risiken wirksam zu minimieren. Besonders empfehlenswert sind risikoarme Lösungen wie lokale Sprachplattformen, die zur Unterstützung von Übersetzungen in der grenzüberschreitenden Kommunikation entwickelt wurden, kompromisslos auf ihre sprachliche Korrektheit überprüft wurden und in einer sicheren, zertifizierten digitalen Umgebung funktionieren. Dieser Ansatz wird es ermöglichen, Vertrauen in der Gesellschaft aufzubauen, die Praktiken der deutsch-polnischen Zusammenarbeit schrittweise zu verbessern und den Boden für die spätere Einführung komplexerer Systeme mit hohem Risiko besser vorzubereiten.

10. Der Katalog der Gefahren, die das Gebiet der beiden miteinander verbundenen Städte betreffen, ist identisch, während die Herangehensweise an die Minimierung oder Beseitigung dieser Gefahren unterschiedlich ist. Diese Unterschiede zeigen sich bereits auf der Ebene der Rechtsgrundlagen für die Funktionsweise der für Krisenmaßnahmen zuständigen Strukturen und führen zu unzureichenden Entscheidungsstrukturen. Es ist daher zu empfehlen, die Zusammenarbeit auf die Arbeitsebene zu verlagern und dabei die in der Europäischen Union bekannte offene Koordinierungsmethode (OKM) anzuwenden. Ein wichtiger Faktor, der zu einer Intensivierung der Maßnahmen drängt, ist die Zeit und die außergewöhnlichen Umstände, die sich aus dem anhaltenden umfassenden Konflikt in der Ukraine ergeben.

11. Die Befragten wiesen auf diejenigen KI-Funktionen hin, die ihnen die Ausführung ihrer Aufgaben nicht abnehmen, sondern sie dabei potenziell unterstützen sollen. Dies sind vernünftige Erwartungen, denen die Technologie zum Zeitpunkt der Erstellung des Berichts gerecht werden kann. Dazu gehören unter anderem die Unterstützung bei der Identifizierung von Cyber-Bedrohungen, die Visualisierung von Krisensituationen sowie die Erfassung und Analyse einer großen Anzahl von Daten und Variablen, die für Entscheidungen zum Schutz von Eigentum und Humanressourcen erforderlich sind.

12. Das Gesetz über den Bevölkerungsschutz und den Zivilschutz führt neue Lösungen im Bereich der Warnung und Alarmierung ein. Ein weiterer Punkt sind die neuen Regeln für die Organisation und Durchführung von Evakuierungen der Bevölkerung aufgrund verschiedener Gefahren und Umstände, die ihre Gesundheit oder ihr Eigentum gefährden. Es wäre sinnvoll, bereits in dieser Phase Vereinbarungen zwischen den Krisenmanagementstrukturen zu treffen oder zumindest zu beginnen, wie man zusammenarbeiten und sich in bestimmten Gefahrensituationen gegenseitig unterstützen kann. Ausgangspunkt sollte ein gemeinsamer und abgestimmter Katalog von Gefahren sein.

13. Bezugnehmend auf das am 18. Juli 2002 unterzeichnete Abkommen zwischen dem Minister für Inneres und Verwaltung der Republik Polen und dem Ministerium für Inneres des Landes Brandenburg über gegenseitige Hilfe bei Katastrophen, Naturkatastrophen und anderen schweren Unfällen[97] weisen wir auf die mögliche und notwendige Organisation von Arbeitstreffen beider Seiten hin, deren Gegenstand der Austausch von Informationen, die Synchronisierung von Krisenreaktionsplänen, die Identifizierung von Kommunikationsengpässen und die Bewertung von Maßnahmen sein sollte. Ein wichtiger Aspekt solcher Treffen ist, vorausgesetzt, dass die Teilnehmergruppe nicht wechselt, der Aufbau von Beziehungskapital, das die Kommunikation verbessert und Vertrauen schafft. Es ist zu erwarten, dass mit dem Inkrafttreten neuer Rechtsvorschriften in Polen im Bereich des Zivilschutzes und des Katastrophenschutzes der Inhalt dieser Vereinbarung evaluiert und an die neuen rechtlichen und organisatorischen Gegebenheiten angepasst wird. Die zweite Erwartung betrifft die Änderung des pauschalen Charakters dieser Vorschriften und ihre Umsetzung in konkrete Maßnahmen und Formen der Zusammenarbeit.

14. Am Rande der Untersuchungen tauchten Äußerungen von Befragten auf, die den Annahmen der Forschungsgruppe entgegenkamen. Sie betrafen die notwendige Änderung der Sichtweise

97 Vereinbarung zwischen dem Innenminister..., op. cit.

auf grenzüberschreitende Regionen im deutschen und polnischen Kommunikations- und Krisenmanagementsystem. Es ist notwendig, diesen Bereich aus der Perspektive des funktionalen Raums der beiden Städte, des Wohnorts einer bestimmten Bevölkerungsgruppe und des intensiven Personenverkehrs zu betrachten. Eine solche grenzüberschreitende Perspektive würde es ermöglichen, auf der Grundlage einer vergleichenden Analyse die Strukturen der Dienste und Zuständigkeiten zu vergleichen und mögliche Kanäle für die Kommunikation und Krisenreaktion zu erfassen.

ZUSAMMENFASSUNG

Das Projekt „Cross-AI Connect: Strengthening Border Resilience (CAIR)" wurde im polnisch-deutschen Doppelstadtgebiet Słubice–Frankfurt (Oder) im Rahmen des Programms „Resilient Borders" durchgeführt. Sein Ziel war es, die Widerstandsfähigkeit der Grenzgebiete zu stärken, indem die Möglichkeiten des Einsatzes von KI-Tools im Bereich der Kommunikation im grenzüberschreitenden Krisenmanagement untersucht wurden.

Hintergrund

Grenzregionen stehen vor besonderen Herausforderungen: Rechtliche und institutionelle Unterschiede, Sprachbarrieren und das Fehlen einheitlicher Verfahren erschweren eine effektive Zusammenarbeit der Behörden. Krisensituationen – Überschwemmungen, Katastrophen, Umweltgefahren – machen nicht an Landesgrenzen Halt, weshalb eine Zusammenarbeit unbedingt erforderlich ist.

Maßnahmen und Outputs des Projektes

Im Rahmen des CAIR-Projekts:

- wurde eine Analyse der Bedürfnisse und Hindernisse in den Krisenmanagementsystemen auf beiden Seiten der Oder durchgeführt,
- wurden Workshops und Konsultationen unter Beteiligung von Behörden und Verwaltungen durchgeführt,
- wurde das Potenzial von KI-Tools in der grenzüberschreitenden Kommunikation (Übersetzungen, Veröffentlichung von Mitteilungen, Überprüfung von Informationen) getestet,
- wurde die Akzeptanz und das Vertrauen der Behörden gegenüber neuen Technologien bewertet,
- wurden rechtliche, organisatorische und technologische Empfehlungen zur weiteren Umsetzung von KI in der öffentlichen Verwaltung erarbeitet.

Wichtigste Schlussfolgerungen

- Moderne Technologien können die Effizienz und Reaktionsgeschwindigkeit in Krisensituationen erheblich steigern.
- Die grenzüberschreitende Koordinierung erfordert nicht nur technische Instrumente, sondern auch Vertrauen zwischen den Institutionen und einen gemeinsamen Rechtsrahmen.
- Die erarbeiteten Lösungen und Empfehlungen haben Modellcharakter und können in anderen Grenzregionen Europas angewendet werden.

Bedeutung für die europäische Politik

Das CAIR-Projekt bestätigt, dass Investitionen in eine widerstandsfähige grenzüberschreitende Governance eine strategische Dimension haben:

- sie stärken die Sicherheit der Bürger,
- sie verbessern den sozialen und wirtschaftlichen Zusammenhalt und
- sie sind ein Beispiel für bewährte Verfahren, die in der Politik der EU und der Mitgliedstaaten genutzt werden können.

CAIR reagiert nicht nur auf die lokalen Bedürfnisse von Słubice und Frankfurt (Oder), sondern schafft auch einen Mehrwert für die gesamte europäische Gemeinschaft – indem es zeigt, dass die Widerstandsfähigkeit von Grenzen mit Zusammenarbeit beginnt.

LITERATURVERZEICHNIS

Aleksandrowicz T.R., Komunikacja kryzysowa w administracji publicznej, Difin Warszawa 2014.

Arnoldi J., Ryzyko, Wydawnictwo Sic!, Warszawa 2011.

Baradyn M., Kaczmarek T., Malczewski A., Zarządzanie kryzysowe w administracji publicznej, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2010.

Baradyn, M., Górski J., Zalewski A., Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego, Akademia Obrony Narodowej, Warszawa 2010.

Bartkiewicz A., Kogo zwolni sztuczna inteligencja? Jedna kluczowa kompetencja pracownika przyszłości, „Rzeczpospolita. PlusMinus" z dnia 14-15.06.2025.

Błaszczak A., Sztuczna inteligencja zatrudni pracowników i przyzna im premie, „Rzeczpospolita" z dnia 21.07.2025.

Boin A., Hart P., Stern E., Sundelius B., The politics of crisis management: Public leadership under pressure (2nd ed.), Cambridge University Press, Cambridge 2017.

BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist, https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf (Letzter Zugang am: 05.10.2025).

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Krisenmanagement, https://www.bbk.bund.de/DE/Themen/Krisenmanagement/krisenmanagement_node.html (Letzter Zugang am: 06.09.2025).

Burgoon J.K., Guerrero L.K., Floyd K., Nonverbal Communication, Routledge 2016.

Burton-Jeangros C., Epidemics and risk communication: Why are lessons not learned?, [in:] M. Bourrier, N. Brender, C. Burton-Jeangros (red.), Managing the Global Health Response to Epidemics, Routledge, New York 2019.

Byram M., Teaching and assessing intercultural communicative competence, Multilingual Matters, Clevedon 1997.

Cabaj J., Komunikacja kryzysowa jako narzędzie zarządzania bezpieczeństwem, [in:] M. Kubiak (red.), Bezpieczeństwo publiczne w warunkach kryzysu, Difin, Warszawa 2015.

Castells M., Communication power, Oxford University Press, Oxford 2009.

Christiansen T., Jørgensen K.E., Wiener A. (red.), The SAGE handbook of European Union politics, Sage Publications, London 2016.

Christiansen, T., Jørgensen K.E., Wiener A., The social construction of Europe, Sage Publications, London 2016.

Coombs, W.T., Ongoing crisis communication: Planning, managing, and responding (4th ed.), Sage, Thousand Oaks 2012.

Dołzbłasz S., Raczyk A., Projekty współpracy transgranicznej na zewnętrznych i wewnętrznych granicach Unii Europejskiej – przykład Polski, „Studia Regionalne i Lokalne" Nr.3(45)2011.

Dziadkiewicz A., Żuber M., Współdziałanie służb, inspekcji i straży na szczeblu powiatu w sytuacjach nadzwyczajnych zagrożeń, „Historia i Polityka" Nr. 23 (30), 2018.

Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (Gesetz zur Durchführung der KI-Verordnung), https://bmds.bund.de/fileadmin/BMDS/Dokumente/Gesetzesvorhaben/CDR_Anlage1-250911_RefE_KIVO-Durchf%C3%BChrungsgesetz_Entwurf_barrierefrei.pdf (Letzter Zugang am: 06.10.2025).

European Commission, Tackling COVID-19 disinformation – Getting the facts right (JOIN/2020/8 final), Brussels 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0008 (Letzter Zugang am: 06.10.2025).

Friedland L.A., Communication, community, and democracy: Toward a theory of the communicatively integrated community, "Communication Research" Nr. 28(4), 2001.

Fuchs C., Social Media: A Critical Introduction (2nd ed.), Sage, London 2017.

FwDV 100, Feuerwehr-Dienstvorschrift 100, März 1999, https://www.idf.nrw.de/dokumente/wir-ueber-uns/aufgaben-des-idf/fwdv100.pdf (Letzter Zugang am: 05.10.2025).

Georsch H., Kling A. (red,), Kompetent und rechtssicher handeln: Einführung in den Bevölkerungsschutz, Walhalla Fachverlag, Regensburg 2024.

Gesetz über den Brandschutz, die Hilfeleistung und den Katastrophenschutz des Landes Brandenburg (Brandenburgisches Brand- und Katastrophenschutzgesetz – BbgBKG) vom 24. Mai 2004 zuletzt geändert durch Artikel 9 des Gesetzes vom 5. März 2024, https://bravors.brandenburg.de/gesetze/bbgbkg (Letzter Zugang am: 05.10.2025).

Gesetz über den Rettungsdienst im Land Brandenburg (Brandenburgisches Rettungsdienstgesetz - BbgRettG) vom 14. Juli 2008 (GVBl.I/08, [Nr. 10], S.186) zuletzt geändert durch Artikel 4 des Gesetzes vom 20. Juni 2024 (GVBl.I/24, [Nr. 28], S.8), https://bravors.brandenburg.de/gesetze/bbgrettg (Letzter Zugang am: 05.10.2025).

Gesetz zur Marktüberwachung und Innovationsförderung von künstlicher Intelligenz z 11 września 2025 r., Projekt ustawy o systemach sztucznej inteligencji, 02.10.2025, https://legislacja.gov.pl/projekt/12390551/katalog/13087932#13087932 (Letzter Zugang am: 06.10.2025).

Gołębiewski J., Zarządzanie kryzysowe w administracji publicznej, Difin. Warszawa 2002.

Gołębiewski, J., Bezpieczeństwo wewnętrzne państwa: Zarys systemu, Akademia Obrony Narodowej, Warszawa 2002.

Grzegorczyk A., Media jako aktor sytuacji kryzysowych, [in:] M. Karwat, M. Kubiak (red.), Komunikacja w sytuacjach kryzysowych, Elipsa, Warszawa 2012.

Grzegorczyk T., Media w sytuacjach kryzysowych, Wydawnictwo C.H. Beck, Warszawa 2012.

Gu H., Li L., Trust and the governance of pandemic risk: Lessons from the COVID-19 crisis, "Journal of Chinese Governance" Nr. 5(2), 2020.

Gudykunst W.B., Bridging differences: Effective intergroup communication (4th ed.), Sage Publications Inc., Thousand Oaks, London, New Delhi 2004.

Habermas J., Strukturwandel der Öffentlichkeit, Hermann Luchterhand Verlag, Neuwied 1962.

Hafez K., The myth of media globalization, Polity Press, Cambridge 2007.

Hall E.T., Beyond culture, Anchor Books, New York 1976.

Hall E.T., The dance of life: The other dimension of time, Anchor Press, New York 1983.

Heath R.L., O'Hair H.D., Handbook of Risk and Crisis Communication, New York, Routledge 2010.

Hofstede G., Culture's consequences: Comparing values, behaviors, institutions and organizations across nations (2nd ed.), Sage, Thousand Oaks 2001.

Kent M.L., Taylor M., Toward a dialogic theory of public relations, "Public Relations Review" Nr.28(1), 2002.

Laajalahti A., Hyvärinen J., Vos M., Crisis communication competence in co-producing safety with citizen groups, "Social Sciences" Nr.5:13, 2016.

Lustig M.W., Koester J., Intercultural competence: Interpersonal communication across cultures (6th ed.), Allyn & Bacon, Boston 2010.

Malinowski M., COBIT. Zarządzanie IT dla organizacji, https://www.drmalinowski.edu.pl/posts/3249-cobit-zarzadzanie-it-dla-organizacji (Letzter Zugang am: 10.08.2025).

Mazur K., Jeszcze nie musimy bać się AI, „Rzeczpospolita. PlusMinus" z dnia 16-17.08.2025.

Paleczny T., Banaś M., Dialog na pograniczach kultur, Nomos, Kraków 2009.

Palen L., Online social media in crisis events, [in:] Proceedings of the 5th International Conference on e-Social Science, University of Manchester, Manchester 2008.

Popis M., Bajda A., Laskowski D., Wybrane aspekty bezpieczeństwa informacyjnego w systemie reagowania kryzysowego, [in:] G. Sobolewski, D. Majchrzak (red.), Zarządzanie kryzysowe w systemie bezpieczeństwa narodowego, Akademia Obrony Narodowej, Warszawa 2011.

Porozumienie między Ministrem Spraw Wewnętrznych i Administracji Rzeczypospolitej Polskiej a Ministerstwem Spraw Wewnętrznych Brandenburgii o wzajemnej pomocy podczas katastrof, klęsk żywiołowych i innych poważnych wypadków, sporządzone w Słubicach dnia 18 lipca 2002 r., M.P. 2003 Nr.15 poz. 211, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20030150211/O/M20030211.pdf (Letzter Zugang am: 06.10.2025).

Raport operacji FENIKS (źródło własne).

Robertson R., Globalization: Social theory and global culture, Sage, London 1998.

Rosyjskie drony nad Polską. Najnowsze informacje z ostatnich godzin (podsumowanie), onet.pl, 11.09.2025, https://wiadomosci.onet.pl/kraj/rosyjskie-drony-nad-polska-najnowsze-informacje-z-ostatnich-godzin-podsumowanie/47hhlx8 (Letzter Zugang am: 11.09.2025).

Rozporządzenie 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-

komunikacyjnych oraz uchylenia rozporządzenia (UE) Nr.526/2013, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32019R0881 (Letzter Zugang am: 06.10.2025).

Rozporządzenie 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) Nr.168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L_202402847 (Letzter Zugang am: 06.10.2025).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG), art. 4 pkt 11, Dz.U. L 119 z 4.5.2016, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679 (Letzter Zugang am: 06.10.2025).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) Nr.300/2008, (UE) Nr.167/2013, (UE) Nr.168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG), Dz.U. L, 2024/1689, 12.7.2024, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L_202401689 (Letzter Zugang am: 06.10.2025).

Seifert J., Information as a strategic resource: Implications for security and policy, "Information & Security" Nr.10(1), 2002.

Seifert J.W., The effects of information technology on governance: A theoretical perspective, Congressional Research Service, Washington DC 2002.

Sienkiewicz-Małyjurek K., Zarządzanie kryzysowe w administracji publicznej. Teoria i praktyka, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice 2015.

Sobera T., Profesjonalizacja komunikowania w sytuacji kryzysowej, Difin, Warszawa 2023.

Sturges D.L., Communicating through crisis: A strategy for organizational survival, "Management Communication Quarterly" Nr.7(3), 1994.

Thomosn C., Hopkin P., Podstawy zarządzania ryzykiem. Jak wdrażać efektywne systemy zarządzania ryzykiem w przedsiębiorstwie, Wydawnictwo Helio, Warszawa 2024.

Traktat między Rzecząpospolitą Polską a Republiką Federalną Niemiec o dobrym sąsiedztwie i przyjaznej współpracy, podpisany w Bonn dnia 17 czerwca 1991 r., Dz. U. z 1992 r. Nr.14, poz. 56.

Trompenaars F., Hampden-Turner C., Riding the waves of culture: Understanding diversity in global business (2nd ed.), Nicholas Brealey Publishing, London 1997.

Tyrała P., Zarządzanie kryzysowe: Teoria i praktyka, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2001.

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny, Dz.U. z 2022 poz. 655, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20220000655/U/D20220655Lj.pdf (Letzter Zugang am: 06.10.2025).

Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, Dz.U. z 1967 Nr.44 poz. 220, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19670440220/U/D19670220Lj.pdf (Letzter Zugang am: 06.10.2025).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2023 poz. 122, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230000122/U/D20230122Lj.pdf (Letzter Zugang am: 06.10.2025).

Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, Dz.U. z 2024 poz. 1907, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20240001907/O/D20241907.pdf (Letzter Zugang am: 06.10.2025).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. z 2018 poz. 1560.

Ustawa Zasadnicza dla Republiki Federalnej Niemiec, https://www.btg-bestellservice.de/pdf/80205000.pdf (Letzter Zugang am: 05.10.2025).

Verordnung über die Einheiten und Einrichtungen des Katastrophenschutzes (Katastrophenschutzverordnung – KatSV) vom 17. Oktober 2012 (GVBl.II/12, [Nr. 87]) zuletzt geändert durch Verordnung vom 16. Dezember 2021 (GVBl.II/21, [Nr. 102], S. ber. GVBl.II/22 [Nr. 31]), https://bravors.brandenburg.de/verordnungen/katsv (Letzter Zugang am: 05.10.2025).

Wnuk-Lipiński E., Świat między kryzysem a nadzieją, Scholar, Warszawa 2004.

Wnuk-Lipiński E., Świat międzyepoki. Globalizacja, demokracja, państwo narodowe, Scholar, Warszawa 2004.

Zivilschutz- und Katastrophenhilfegesetz vom 25. März 1997 (BGBl. I S. 726), das zuletzt durch Artikel 144 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, https://www.gesetze-im-internet.de/zsg/ZSKG.pdf (Letzter Zugang am: 05.10.2025).

VERZEICHNIS DER ABBILDUNGEN, TABELLEN UND DIAGRAMME

Tabelle 1. Beispielhafte Anwendung der RACI-Matrix für den Bereich der Doppelstadt Słubice und Frankfurt (Oder) 7
Abbildung 1. Die wichtigsten Grundsätze von COBIT 5 9
Tabelle 2. Interkulturelle Kommunikation im deutsch-polnischen Grenzgebiet 28
Tabelle 3. Modelle für das Krisenkommunikationsmanagement 29
Tabelle 4. Typologie der Mitteilungen – Merkmale 31
Tabelle 5. Krisenkommunikation in den Kommunalverwaltungen Polens und Deutschlands 32
Tabelle 6. Barrieren in der interkulturellen Kommunikation im Krisenmanagement 33
Tabelle 7. Vertrauen in Informationsquellen in Krisensituationen 33
Tabelle 8. Funktionen der Medien in Krisensituationen 34
Tabelle 9. Vorteile und Risiken der Digitalisierung der Krisenkommunikation 35
Tabelle 10. Nutzung digitaler Medien in der Krisenkommunikation (Polen–Deutschland) 35
Tabelle 11. Digitale Krisenkommunikation im Sinne von Hall (hoher und niedriger Kontext) 35
Tabelle 12. Hofstedes Kulturdimensionen und Krisenkommunikation (Polen-Deutschland) 38
Tabelle 13. Trompenaars kulturelle Dimensionen und Krisenkommunikation (Polen-Deutschland) 39
Tabelle 14. Kulturelle Dimensionen von GLOBE und Krisenkommunikation (Polen-Deutschland) 40
Abbildung 2. Zusammenhang zwischen Krisenmanagement, Katastrophenschutz und Zivilschutz 64
Abbildung 3: Nutzung von KI-Tools am Arbeitsplatz durch die Befragten 82
Diagramm 1. Von den Befragten erwartete Funktionen des Führungsunterstützungssystems, die bei der Ausübung ihrer dienstlichen Aufgaben wünschenswert sind 85
Diagramm 2. Erwartete KI-Funktionen, die am Arbeitsplatz der Befragten nützlich sind 86
Abbildung 4. Arten von Cybersicherheitsvorfällen, von denen die Befragten in letzter Zeit gehört haben 86
Diagramm 3. Wahrgenommene Cybersicherheitsrisiken am Arbeitsplatz der Befragten aus Polen 87
Diagramm 4. Wahrgenommene Cybersicherheitsrisiken am Arbeitsplatz der Befragten aus Deutschland 88

BIOGRAMME

Agnieszka Bielawska – Habilitierte Doktorin der Sozialwissenschaften in der Disziplin Politik- und Verwaltungswissenschaften (2020), Doktorin der Geisteswissenschaften im Bereich Politikwissenschaft (2007). Sie absolvierte ihr Promotionsstudium am Institut für Politikwissenschaft und Journalistik der Adam-Mickiewicz-Universität Posen sowie ein postgraduales Studium im Bereich Europäische Verwaltung an der Fachhochschule für Verwaltung und Rechtpflege in Berlin / Adam-Mickiewicz-Universität Posen. Sie war Stipendiatin des Kontaktstipendiums des DAAD sowie der Universität Potsdam. Sie ist Mitglied der Polnischen Gesellschaft für Europastudien und der Polnischen Gesellschaft für Politikwissenschaft. Sie ist Sekretärin des Jahrbuchs für Europäische Integration (Rocznik Integracji Europejskiej). Ihre Forschungsschwerpunkte sind die Europapolitik der deutschen Christdemokraten (CDU/CSU), die Europäische Integration sowie die deutsch-polnischen Beziehungen. Sie ist Autorin zahlreicher Publikationen zu dieser Thematik.

Ilona Biernacka-Ligięza – Universitätsprofessorin. Sie ist verbunden mit der Maria-Curie-Skłodowska-Universität in Lublin, der Karls-Universität in Prag sowie der ANS in Wałbrzych. Sie war Gastprofessorin an der University of North Carolina, der Universität Macerata, der Canterbury Christ Church University sowie der Universität Oslo. Sie arbeitet als bewertende Expertin für zahlreiche Programme der Europäischen Kommission. Sie hat über 20 Forschungsstipendien erhalten, darunter 15 internationale. Sie koordinierte Projekte im Rahmen von Programmen wie: Horizon 2020, Horizon Europe, Fulbright, EOG (EWR), Visegrad. Sie erhielt ein individuelles Marie Skłodowska-Curie-Stipendium. Sie veröffentlichte 10 Monographien und über 100 wissenschaftliche Artikel sowie Buchkapitel. Ihre Forschungsinteressen umfassen: lokale Medien, Massenkommunikation, digitale Medien, interkulturelle Kommunikation, lokale Demokratie, Globalisierung, Glokalisierung, Medien und Politik, Medien und Identität, Minderheiten in der lokalen Öffentlichkeit, Gesundheitskommunikation. Aktuell konzentriert sie sich in ihrer Forschung auf die Aspekte des Digitalisierungsprozesses der Gesundheitskommunikation, insbesondere im Kontext des aktiven Alterns. Der zweite Bereich ihrer jüngsten Forschung sind die Herausforderungen der strategischen Kommunikation, hauptsächlich im komparativen Aspekt.

Dariusz Dymek – Doktor der Sozialwissenschaften, Oberdozent an der Adam-Mickiewicz-Universität Posen, Spezialist auf dem Gebiet des Bevölkerungsschutzes und Krisenmanagements. Er ist Absolvent der Höheren Offiziersschule für Funktechnik in Jelenia Góra, der Universität Stettin (Masterstudium), der Hauptschule des Feuerwehrdienstes (Aufbaustudium in Krisenmanagement), der Adam-Mickiewicz-Universität Posen (Aufbaustudium in Verwaltung sowie Promotion in Sozialwissenschaften, Fachgebiet Sicherheitspolitik). Er ist Autor wissenschaftlicher und publizistischer Artikel im Bereich Krisenmanagement, Bevölkerungsschutz und Innere Sicherheit, sowie Teilnehmer zahlreicher wissenschaftlicher Konferenzen. Seit 2004 ist er Direktor der Abteilung für Sicherheit und Krisenmanagement im Woiwodschaftsamt Großpolen in Posen. Im Jahr 2024 nahm er an den Arbeiten des Krisenstabs in der Gemeinde Lądek-Zdrój (Bad Landeck) teil, die von den Folgen des Septemberhochwassers betroffen war, und fungierte als Berater des Bevollmächtigten des Ministers für Innere Angelegenheiten und Verwaltung zur Leitung der Maßnahmen zur Verhinderung und Beseitigung der Hochwasserfolgen in den Gemeinden Lądek-Zdrój und Stronie Śląskie (Seitenberg).

Damian Flisak – Doktor der Rechtswissenschaften (Ludwig-Maximilians-Universität München), LL.M., Rechtsberater mit mehr als zehn Jahren praktischer Erfahrung, Mitglied des Expertennetzwerks

Team Europe Direct der Europäischen Kommission im Bereich KI, Of Counsel in der Kanzlei Lubasz i Wspólnicy, Mitbegründer des Think Tanks Blue Dragon Institut. Neben der Rechtsberatung betreibt er professionelle Regulierungsberatung (Public Affairs), hat mehrfach nationale und EU-Gesetzesentwürfe begutachtet und war an der Mitgestaltung der Strategie zur Entwicklung der KI in Polen beteiligt. Er hält Vorlesungen an der Landesrichterschule und Staatsanwaltschaft (Krajowa Szkoła Sądownictwa i Prokuratury) sowie für Richterpersonal am Gerichtshof der Europäischen Union in Luxemburg. Er ist Dozent für Recht der Künstlichen Intelligenz und Geistiges Eigentum an der Leon Koźmiński Akademie, der Polnisch-Japanischen Akademie für Computertechnik, am Institut für Rechtswissenschaften der Polnischen Akademie der Wissenschaften (PAN) und an der Warsaw School of Economics (Szkoła Główna Handlowa). Er ist vereidigter Übersetzer der deutschen Sprache und Mitautor eines der größten Deutsch-Polnischen Wörterbücher.

Konrad Glejt – Absolvent führender Hochschulen in Posen und Warschau. Enthusiast für Cybersicherheitsfragen. Beruflich spezialisiert er sich auf die Bereiche Cloud Security, Windows- und macOS-Betriebssysteme sowie auf Schulungsmaßnahmen zu Bedrohungen im Netz und Schutzmöglichkeiten davor. Berufserfahrung sammelte er im größten polnischen Pharmaunternehmen sowie in einer Staatseigentumsgesellschaft aus dem Energiesektor. Er sicherte die kritische Infrastruktur des Staates unter Umsetzung der Richtlinien und Empfehlungen der Aufsichtsbehörden. Er verfügt über Erfahrung aus einem internationalen Unternehmen der FMCG-Branche, das über 20.000 Mitarbeiter beschäftigt. Er baut seine eigene Marke unter dem Namen *cybear* auf, schult Organisationen und erstellt Video-Materialien zur Sicherheit im Netz. Eines seiner bevorzugten Branchenzitate lautet: „Es ist nicht die Frage, ob du gehackt wirst, sondern wann es passiert." Privat ist er Liebhaber von Reisen sowie aktiver Freizeitgestaltung und gutem Audio-Equipment.

Adam Jaskulski – Doktor der Sozialwissenschaften im Bereich Politikwissenschaft sowie Rechtsanwalt, Politologe und Jurist. Absolvent der Fakultät für Recht und Verwaltung sowie des Instituts für Politikwissenschaft und Journalistik der Adam-Mickiewicz-Universität Posen. Seit 2011 ist er Mitglied der Großpolnischen Rechtsanwaltskammer. Derzeit ist er Assistenzprofessor an der Abteilung für Lokale Macht- und Selbstverwaltungsforschung der Fakultät für Politikwissenschaft und Journalistik der UAM Posen, wo er unter anderem Lehrveranstaltungen zu Europäischer Integration, EU-Institutionen und -Recht sowie EU-Wirtschaftsrecht und materiellem Strafrecht hält. Seine Forschungsinteressen umfassen: Institutionen der Europäischen Union, Gemeinsame Außen- und Sicherheitspolitik der EU, Europarecht, EU-Verkehrspolitik, Theorien der Europäischen Integration, Euroskeptizismus, polnische Europapolitik, Brexit, gesellschaftliche Partizipation, partizipative Demokratie, lokale Selbstverwaltung auf Gemeindeebene. Er ist Autor von über 20 wissenschaftlichen Artikeln aus dem Bereich der Politikwissenschaften und des Rechts. Neben seiner beruflichen Tätigkeit engagiert er sich in der Arbeit des Zentrums für Europäische Forschung und Bildung in Posen, wo er die Funktion des stellvertretenden Vorstandsvorsitzenden innehat. Er arbeitete fünf Jahre lang mit der lokalen Selbstverwaltung zusammen und leistete Rechtsbeistand. Er verfügt über Erfahrungen in der Implementierung der DSGVO seit 2018. E-Mail: adam.jaskulski@amu.edu.pl.

Marcin Krzymuski – Doktor der Rechtswissenschaften, Mitarbeiter der Stadtverwaltung in Frankfurt an der Oder (Project Manager im Frankfurt-Slubicer Kooperationszentrum). Zuvor war er viele Jahre lang wissenschaftlicher Mitarbeiter an der Europa-Universität Viadrina in Frankfurt (Oder) (Projektleiter des Projekts „Kompetenzzentrum EVTZ" im Rahmen des „Viadrina Center B/Orders in

Motion“). Er ist Rechtsberater (radca prawny) in Polen. Er beschäftigt sich hauptsächlich mit rechtlichen Fragestellungen der grenzüberschreitenden Zusammenarbeit öffentlicher Einrichtungen.

Mikołaj Tomaszyk – Habilitierter Doktor (Dr. habil.), Professor der UAM, Politologe, Absolvent der Studiengänge Management und Theologie. Er leitet die Lubońer Universität des Dritten Lebensalters (Uniwersytet Luboński III Wieku) und ist ein Enthusiast der Wissenschaftspopularisierung. Er ist Experte in Projekten, die aus EU-Mitteln kofinanziert werden. Seine wissenschaftlichen Interessen umfassen: Sicherheit in der Stadt, Stadttheorie, städtische Verkehrspolitik, lokale Selbstverwaltung (Kommunalverwaltung), Ethik der Sorge (Care-Ethik). E-Mail: mikolaj.tomaszyk@amu.edu.pl .