Band 6 / 2023

Zukünftige Technologien im Kontext hybrider Bedrohungen

Das Hybrid Threat Meta Monitoring Modell (HTM3)

Anton Dengg, Joachim Klerx, Klaus Mak, Andreas Peer

Schriftenreihe der
Landesverteidigungsakademie

UNSER HEER

Schriftenreihe der
Landesverteidigungsakademie

Anton Dengg, Joachim Klerx, Klaus Mak, Andreas Peer

Zukünftige Technologien im Kontext hybrider Bedrohungen

Das Hybrid Threat Meta Monitoring Modell (HTM3)

6/2023
Wien, Juli 2023

Impressum:

Medieninhaber, Herausgeber, Hersteller:
Republik Österreich / Bundesministerium für Landesverteidigung
Rossauer Lände 1
1090 Wien

Redaktion:
Landesverteidigungsakademie
Zentraldokumentation
Stiftgasse 2a
1070 Wien

Schriftenreihe der Landesverteidigungsakademie

Juli 2023
ISBN 978-3-903359-72-7

Druck:
ReproZ W 23-3521
Stiftgasse 2a
1070 Wien

Inhaltsverzeichnis

Zukünftige Technologien im Kontext hybrider Bedrohungen

Das Hybrid Threat Meta Monitoring Modell (HTM3)

Vorwort

Für staatliche wie europäische Sicherheit ist eine vorausschauende und umfassende sicherheitspolitische Analyse von zentraler Bedeutung. Sorgfältig ausgearbeitete Bedrohungsszenarien sind dabei ein wesentliches Element. Diese werden immer komplexer und umfassen schon seit längerem multidimensionale hybride Konfliktbilder.

Hybride Bedrohungen sind per se keine neue Form von Beeinflussungsmöglichkeiten. Ins europäische Bewusstsein rückte diese Art der Machtprojektion vor allem mit der Einnahme der Krim durch russische Kräfte im Jahr 2014. Seit dieser Zeit haben sich die Möglichkeiten hybrider Austragung von Konflikten quantitativ wie qualitativ weiter verbreitert. Zunehmend komplexer werdende hybride Bedrohungsansätze, bei denen neue technologische Entwicklungen eine hohe Relevanz haben, sind von wesentlicher Bedeutung. Neue Technologien werden zu immer mächtigeren Werkzeugen der Einflussnahme und Machtprojektion. Sie stellen sicherheitspolitische und militärische Analysen sowie Entscheidungsträger vor immer schwieriger werdende Herausforderungen. Unübersichtlichkeit und Komplexität sind prägende Charakteristika der gegenwärtigen Sicherheitslage. Daher braucht es konsequenterweise auch neue Werkzeuge, Methoden und Tools, die Analyse- und Entscheidungsprozesse unterstützen.

Genau hier setzen die Autoren mit ihrer Arbeit an. Durch einen speziell entwickelten innovativen Analyseansatz betreten die Forscher Neuland.

Es wird versucht, zukünftige Herausforderungen auf dem Gebiet hybrider Bedrohungen mit größerer Treffsicherheit und Objektivität zu analysieren. Dabei werden zunächst computergestützt sicherheitsbedenkliche Aktivitäten, bei denen Technologie eine Rolle spielt, vorgefiltert. Die jeweiligen Fachexperten beurteilen alsdann die verfügbaren Informationen und übertragen ihre Ergebnisse in ein Lagebild, das zukunftsorientiert und an möglichst präventiver Entscheidungsfindung orientiert ist.

Oberstes Ziel ist es, multidimensionale hybride Ansätze, deren vorrangiges Ziel es ist, unter der Schwelle gewaltsamer Auseinandersetzungen zu bleiben, frühzeitig zu erkennen. Der Zweck des Modells ist es, eine rechtzeitige Einleitung von umfassenden und zielgerichteten Gegenmaßnahmen in allen Domänen und für alle relevanten Institutionen zu erleichtern.

In einem weiteren Schritt ist angedacht, aktuell noch analog ausgeführte Analyseschritte durch künstliche Intelligenz zu unterstützen, sodass Experten sich auf ihre eigentliche Kernaufgabe - das Finden innovativer Gegenstrategien - konzentrieren können.

Ich gratuliere den Autoren zur Arbeit und wünsche der interessierten Leserschaft Freude beim Durcharbeiten dieser Publikation.

General Mag Robert BRIEGER
Vorsitzender des Militärausschusses der Europäischen Union

Kurzfassung/Abstract

Hybride Bedrohungen beschäftigen weltweit Sicherheitspolitiker. Aufgrund unzähliger neuer, zum Teil technologischer Machtmittel und deren Amalgamierung hat sich ein komplexes Bedrohungsbild gebildet. Dies findet mitunter in kreativer und überraschender Art und Weise statt. Daher sind Experten bemüht, entsprechende Analyseverfahren zu entwickeln.

Ein Projekt des Instituts für Friedenssicherung und Konfliktmanagement (IFK) der Landesverteidigungsakademie (LVAk) in Kooperation mit der Zentraldokumentation (ZentDok) der LVAk sowie mit einem Vertreter des Austrian Institute of Technology (AIT) realisierte ein derartiges Analyse-Modell.

Erstmalig wird mit dem in dieser Publikation vorgestellten Meta-Modell ein Horizon Scanning und ein iteratives Analysesystem mit Hilfe einer kollaborativen gesamtstaatlichen Wissensgenerierung eine systematische Erfassung, Strukturierung und Visualisierung hybrider Bedrohungen im Kontext unkonventioneller Kriegsführung ermöglicht. Bisherige Analysen stützten sich auf eher unstrukturierte Informationsdatenbanken. Das erarbeitete Modell lässt nunmehr eine strukturierte Datenerfassung zu, um mögliche Bedrohungstrends zu visualisieren und einen frühzeitigen, gesamtstaatlichen und strategischen Handlungsbedarf zu identifizieren und dokumentieren. Daraus ergeben sich entsprechende mögliche staatliche Handlungsoptionen nach Prioritäten.

Bedrohungs- und Handlungsperzeptionen sind mitunter unterschiedlich gewichtet. In Staaten herrschen durchaus uneinheitliche Gegebenheiten vor. Die Flexibilität des Meta-Modells nimmt darauf Rücksicht

und lässt für den jeweiligen Anwender eine maßgeschneiderte Bedarfskonfiguration zu.

Hybrid threats are at the forefront of security policy concerns globally. The emergence of diverse, largely technological power mechanisms and their fusion has created an intricate threat landscape, relevant analytical methodologies and improved procedures.

A project initiated by the Institute for Peacekeeping and Conflict Management (IFK) of the National Defense Academy (LVAk), in cooperation with the Central Documentation (ZentDok) of the LVAk and a delegate from the Austrian Institute of Technology (AIT), developed such an analytical model.

The meta-model presented in this publication is a progressive, iterative system for scanning the horizon, utilizing a comprehensive, government-wide knowledge generation process to systematically identify, organize and visualize hybrid threats within the created framework of unconventional warfare. Traditional analyses have relied on somewhat less organized data sets with a minor focus on proactive strategic planning. The newly created model facilitates a structured data collection approach, enabling visualization of potential threat trends, early detection and documentation of required intervention at both national and strategic levels, which subsequently inform feasible state response strategies based on clearly identified priorities.

Up to now, perceptions of threats and subsequent actions vary, often weighed differently across nations. The situation between different EU countries is often inconsistent to each other. The proposed meta-model accommodates these discrepancies by permitting tailored requirement configurations for national strategic and tactical needs and at the same time prepares for future automatization with artificial intelligence.

1. Einleitung

Technologien ermöglichen direkte und indirekte staatliche wie nichtstaatliche Machtprojektionsmöglichkeiten. Verbesserte Technik ermöglicht Akteuren - nachteilig intendiert - einen anderen Akteur noch zielgerichteter und manipulativer zu beeinflussen. Technologie stellt somit für „angegriffene" Staaten vermehrt eine hybride Bedrohung (HB) und eine sicherheitspolitische Herausforderung dar. Künstliche Intelligenz (KI) wird dies negativ wie positiv verstärken. So z.B. ist Christine Wahlmüller-Schiller überzeugt: *„Die durch KI bevorstehenden Veränderungen sind fundamental und unumkehrbar. Sie haben Auswirkungen auf den Einzelnen und die Gesellschaft, das soziale Gefüge, den Wert und die Gestaltung der Arbeit sowie auf die politische Willens- und Meinungsfreiheit"*[1]. Diese Einschätzung wird ebenso Sicherheitskräfte betreffen. Hier wird KI sowohl Vor- als auch Nachteile - d.h. als Abwehr- und/oder. als Angriffskomponente - mit sich bringen. Der Einsatz intelligenter Systeme wird eine immer entscheidendere Rolle in den Bereichen Politik, Wirtschaft, der Informationstechnologie und bei Streitkräften im In- und im Ausland und insbesondere beim internationalen Krisen- und Konfliktmanagement (IKKM) spielen. Der Einfluss auf weiterer Domänen hybrider Bedrohungen ist nicht auszuschließen. Völker- wie menschenrechtliche Aspekte auf nationaler und internationaler Ebene sind daher ebenso zu beleuchten.

Sicherheitskräfte könnten durch den Einsatz unterschiedlicher Arten neuer Technologien - vor allem bei Missionen im Rahmen des Internationalen Krisen- und Konfliktmanagement (IKKM) - Ziel derartiger hybrider Bedrohungen werden. Rückwirkungen auf Entsendestaaten sind jedenfalls vorstellbar. Neue Technologien hatten stets einen starken Einfluss auf staatliche Bedro-

[1] Christine Wahlmüller-Schiller, Künstliche Intelligenz - wohin geht die Reise. In: „Elektrotechnik & Informationstechnik", published: 25 October 2017, S. 364-369

hungsszenarien und werden Konflikte und Kriege zukünftig noch gravierender prägen. Eine mögliche Strategie bei hybriden Bedrohungen ist, eine gesteuerte Gefährdung im Inland, angefacht durch einen ausländischen Akteur, zu erwirken. Das Gebot der Stunde ist, sich tunlichst frühzeitig mit dieser Materie zu befassen, Analysemodelle zu generieren, um sich zeitgerecht und damit präventiv auf die neuen Herausforderungen einzustellen. Dadurch wird Staaten ermöglicht, deren Handlungsfähigkeit zu erhalten bzw. zu stärken.

Das Institut für Friedenssicherung und Konfliktmanagement (IFK) der Landesverteidigungsakademie (LVAk) Wien, beschäftigt sich schon seit 2011 mit möglichen neuen Formen staatlicher Machtprojektionsmöglichkeiten. Mit 2012 wurde der Fokus auf theoretische Aspekte hybrider Bedrohungen gelegt. Ergebnisse wurden erstmalig 2015[2] bzw. 2016 in deutscher[3] und englischer[4] Sprache publiziert. Seit 2016 beschäftigen sich Forscher am IFK mit Sonderaspekten hybrider Bedrohungen: Technologie und deren negativer Anwendungsfelder sowie positiver Einflussmöglichkeiten auf Staat und Gesellschaft.[5] Auf diese bisherigen IFK-Forschungsergebnisse zu Machtdefinition und Bedrohungsperzeptionen stützt sich die vorliegende Arbeit.

Seit 2020 konzentriert sich das IFK, gemeinsam mit der Abteilung Zentraldokumentation (ZentDok) der LVAk sowie dem Austrian Institut of Technology (AIT), im Projekt „Zukünftige Technologien im Kontext hybrider

[2] Anton Dengg, Michael Schurian (Hrsg.), Vernetzte Unsicherheit - Hybride Bedrohungen im 21. Jahrhundert, Schriftenreihe der Landesverteidigungsakademie, Band 15/2016, Wien, Juli 2015

[3] Anton Dengg, Michael Schurian (Hrsg.), Vernetzte Unsicherheit - Hybride Bedrohungen im 21. Jahrhundert, 2. überarbeitete und erweiterte Auflage, Schriftenreihe der Landesverteidigungsakademie, Band 6/2016, Wien, Februar 2016

[4] Anton Dengg, Michael Schurian (Eds.), Networked Insecurity - Hybrid Threats in the 21st Century, Schriftenreihe der Landesverteidigungsakademie, Band 17/2016, Wien, Februar 2016

[5] Anton Dengg (Ed.), Tomorrow's Technology. A Double-Edged Sword, Schriftenreihe der Landesverteidigungsakademie, Band 3/2018, Vienna, March 2018

Bedrohungen und deren sicherheitspolitischer Auswirkungen auf Staat, Gesellschaft und Sicherheitskräfte - Risiken und Lösungsansätze" auf modellhafte Analysevarianten. Dabei wird untersucht, inwieweit Aktivitäten mithilfe von Spitzentechnologien von aggressiven Akteuren für den eigenen Staat souveränitätsgefährdend sein könnten.

Die ZentDok als Wissensplattform des österreichischen Bundesheeres (ÖBH) ist grundsätzlich verantwortlich für die Bereitstellung von Open Source-Fachinformationen für alle Dienststellen des ÖBH. Des Weiteren obliegen der ZentDok Aufgaben im Bereich des Wissensmanagements und der Wissensentwicklung sowie der Betrieb eines Cyber-Dokumentations- und Forschungszentrums. Eine wesentliche Rolle ist dabei das zur Verfügung stellen aktueller Open-Source Produkte für Lagebilder, sowie die Durchführung und Mitarbeit an Forschungs- und Entwicklungsprojekten.

In die gegenständliche Arbeit fließen langjährige Erfahrungen im Open Source Intelligence (OSINT) sowie Wissens- und Modellentwicklungsbereich aus bisherigen Use-Cases und Projektbeteiligungen ein. Dabei handelt es sich neben BMLV- (Bundesministerium für Landesverteidigung), insbesondere um KIRAS[6]-, EDA[7]- bzw. EU-Projekte[8]. Dies ist in offiziellen Publikationen und in der internen ZentDok-Wissensmanagement-Datenbank Adonis/Promote in Form interaktiver Modelle und Prozesslandschaften dokumentiert. Die Expertisen wie z.B. bei der Recherche oder Analyse sowie

[6] Das österreichische Förderungsprogramm für Sicherheitsforschung -KIRAS- unterstützt nationale Forschungsvorhaben, deren Ergebnisse dazu beitragen, die Sicherheit - als dauerhafte Gewährleistung eines hohen Niveaus an Lebensgrundlagen und Entfaltungsmöglichkeiten - für alle Mitglieder der Gesellschaft zu erhöhen.

[7] The European Defence Agency was established under a Joint Action of the Council of Ministers on 12 July, 2004, "to support the Member States and the Council in their effort to improve European Defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future".

[8] H2020 (Horizon 2020) bzw. HEU (Horizon Europe) sind die relevanten Forschungsprogramme der Europäischen Kommission.

bei der Modellierung und Wissensentwicklung wurden im Projekt mannigfaltig angewandt.

Das AIT trug wesentlich mit Expertenwissen sowie Use Case Daten aus dem CATALYST (ColAborative Trend AnaLYtics SysTem) Repository und mit Ergebnissen aus verschiedenen EDA-Projekten zur Modellentwicklung bei.

Generell ist festzuhalten, dass auf die Datenaufbereitung und die damit zusammenhängenden Möglichkeiten bei der sicherheitspolitischen Analyse ein besonderes Augenmerk zu richten ist. Akteure, die mit Hilfe oder/und in Kombination von künstlicher Intelligenz (KI) derartige Auswertungen beherrschen, werden die Hoheit über die Machtprojektion, aber auch bei der Resilienz innehaben.

1.1. Problemstellung

Betrachtet man Bedrohung als Gefährdung der Sicherheit, so sind unterschiedliche Dimensionen festzumachen. Beispielsweise können diverse Gefährdungen wahrgenommen werden, wenn solche vorhanden sind. Eine Gefährdung kann aber ebenso subjektiv empfunden werden, obwohl diese nicht existiert. Vorstellbar ist, dass keine Gefährdung wahrgenommen wird, obgleich diese existiert.[9] Die Gründe dafür sind vielfältig.

Bedrohungsperzeptionen werden dadurch erschwert, falls sich ein negativ gesinntes Gegenüber mit Hilfe hybrider Strategien sowohl der „Soft-" als auch der „Hardpower" bedient. Insbesondere bei der Anwendung von Soft-

[9] vgl. Thomas Pankratz, „Überlegungen zum Begriff „Strategische Bedrohungen", in: Anton Dengg, Michael Schurian (Hrsg.), Vernetzte Unsicherheit - Hybride Bedrohungen im 21. Jahrhundert, 2. überarbeitete und erweiterte Auflage, Schriftenreihe der Landesverteidigungsakademie, Band 6/2016, Wien, Februar 2016, S. 18

power ist eine Intention oft kaum zu erkennen bzw. nachzuweisen, da Aggressoren Verschleierungstaktiken einsetzen.

Eine Suche nach dem Topic „hybrid war", auf Google Trends zeigt, dass es einen deutlichen Anstieg des Suchinteresses seit 2013/2014 gibt, im Kontext des Ukraine Konfliktes. Die Nato beschuldigte Russland hybride Taktiken im Ukraine-Konflikt anzuwenden und bezog sich dabei auf ein Konzept, das von Gerasimov 2010[10] veröffentlicht wurde. Betrachtet man das Suchinteresse, so gab es ab 2004 für eine sehr kurze Zeit ein Interesse, anschließend ein zunehmendes Interesse, beginnend mit 2008 und 2013. Das lässt sich dadurch erklären lässt, dass die Primakov Doctrine ein gedanklicher Vorläufer der Gerasimov Konzepte ist.

Die folgende Graphik zeigt neben der Zeitreihe des Suchinteresses zu hybrider Kriegsführung auch die aktuelle (15.3.2022) geographische Verteilung des Suchinteresses and die Übersicht über die globalen Meldungen zur hybriden Kriegsführung.

[10] https://vpk-news.ru/articles/14632

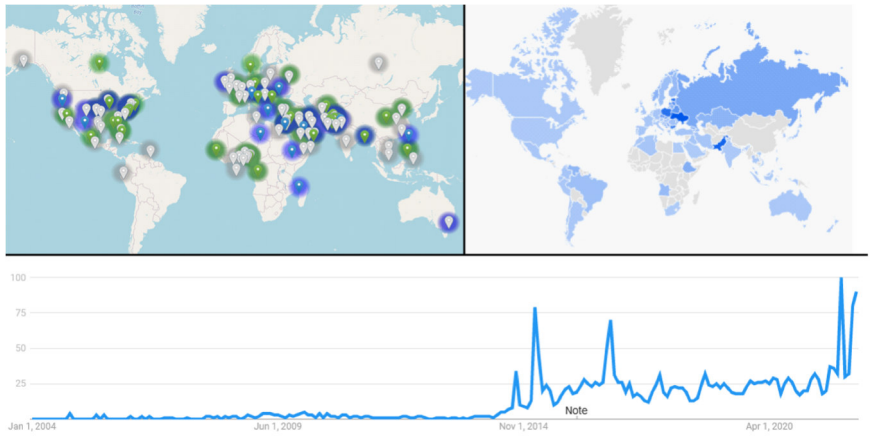


Abbildung 1 –"Hybrid warfare" Ereignisse und das globale Suchinteresse[11]

Die aktuellen Suchergebnisse zeigen, dass ein großes Interesse an hybriden Bedrohungen und entsprechenden Konzepten besteht, besonders in den Ländern der Region um die Ukraine, was nicht überraschend ist. Differenzierter ist die Graphik zu den Pressemeldungen. Die Ergebnisse zeigten einen klaren Zusammenhang zwischen den „unkonventionellen Bedrohungen" und den aktuellen Konfliktherden, inklusive aller direkten und indirekt involvierten Länder. Fasst man alle Meldungen grob zusammen, so gibt diese Tatsache Hinweise auf einen eskalierenden Einsatz von Hard-Power- und Soft-Power-Aktivitäten, um die physische, psychologische, kulturelle, politische und menschliche Dimension des jeweiligen Gegners anzusprechen. Zum Zeitpunkt der Auswahl der Ereignisse für die Pilotanwendung war der Ukraine Konflikt noch nicht eskaliert, weswegen die Auswertung nicht in die Pilotanwendung einfließen konnte. Aus der aktuellen Beobachtung (bis 15.3.2022) der Meldungen zur hybrider Kriegführung ergibt sich ein exponentieller Anstieg, in den letzten Monaten, der eskaliert ist in den Sanktionen

[11] Vgl. CATALYST: A common development effort of AIT and Zentdok; Ausschnitt Google Trends (unten)

und Gegensanktionen im Zuge des Ukraine Konfliktes, neben vielen weiteren hybriden Bedrohungen.

Bei den aktuellen Bedrohungen ist charakteristisch, dass in der Regel unklar ist, wann diese beginnen oder enden. Jede Form von subversiven Taktiken wird verwendet, um einen Vorteil zu erlangen. Viele dieser aktuellen hybriden Taktiken beginnen oft mit Medienmeldungen zu subversiven Aktivitäten nichtstaatlicher Akteure. Terroristische und cyberterroristische Angriffe, einschließlich technologisch fortschrittlicher Systeme, die über ihre ursprünglichen Mittel hinaus (z. B. zivile Drohnen für militärische Zwecke) (missbraucht) verwendet werden, unterstützt durch Propaganda, Medienkontrolle und/oder Desinformationskampagnen, kriminelle Aktivitäten als gemeinsame Finanzierungsquelle oder als angreifen und darauf abzielen, die Gesellschaft zu spalten, ihre Einheit zu untergraben und die Durchführung politischer Entscheidungen zu erschweren.
In den vorliegenden Fällen war es eine gängige Taktik, jedes Völkerrecht zu missachten – und sich subversiver Geheimdienste, Sabotage oder politischer Unterstützung extremistischer Gruppen zu bedienen.

In den friedenserhaltenden Missionen der letzten Jahre haben sich Soft-Power-Aktivitäten in Kombination mit Missionen zu militärischem Schutz als einer der wichtigsten Erfolgsfaktoren zur Lösung von Konflikten erwiesen. In Kombination mit der Digitalisierung der globalen Gesellschaft gilt dies in Zukunft vermutlich in noch stärkere Ausmaße. Die Pilotanwendung von HTM3 dient dazu zu zeigen, wie die entwickelten Modelle zur Planung der Taktik dieser Einsätze beitragen können.

Speziell hybride Bedrohungsanalysen haben nach möglichst objektiven Kriterien und Verfahren zu erfolgen. Experten sind kaum mehr in der Lage die global existierende hohe Anzahl an Publikationen, Ereignissen, Aktivitäten und Meldungen - die in unzähligen Sprachen erschienen (Analysen nicht eingerechnet) - allumfassend zu analysieren. Daher braucht es ein Toolset, um

objektiven Kriterien zu entsprechen. Genau hier setzt das in einem Projekt erarbeitete und in diesem Druckwerk dargelegte Modell an.

Im Projekt war das primäre Ziel des Forscherteams, ein möglichst objektives Analysemodell über zukünftige Technologien im Kontext hybrider Bedrohungen zu entwickeln. Um diese Zielsetzung zu erreichen, bedarf es in weiterer Folge der Zuhilfenahme von KI. Als Zwischenstufe dorthin gilt es, zunächst einen Analyseprozess mit Experten zu entwickeln, um für die operative Anwendung auch für die jeweilige KI genügend Basisdaten zur Verfügung zu haben. Durch eine ausreichende Anzahl von Sachverhaltsverknüpfungen von Ereignissen und möglichen Wirkungen erhält die KI die notwendigen Voraussetzungen für zunächst teilweise selbstständige Analysen.

Generell liegt die Schwierigkeit bei der Entwicklung eines derartigen Analysemodells darin, aufgrund der Unzahl komplexer hybrider Bedrohungsinstrumente – praktischer sowie theoretischer Natur - zunächst entsprechende Parameter für eine Suchfunktion und Vorgaben hinsichtlich einer späteren KI-Anwendung zu generieren. Ohne KI ist es nahezu unmöglich, Suchkriterien für heterogene Machtprojektionsvariationen festzumachen – insbesondere, wenn es sich um weitreichende, umfassende, innovative und komplexe Softpowerkombinationen handelt. Bisher fehlen dafür Instrumente und Methoden. Adäquate Kriterien sind daher zunächst von Experten „intellektuell" zu entwickeln.

Daher wurden zunächst im Laufe des Projektes erste Ergebnisse einem interministeriellen Expertenteam präsentiert, um die Brauchbarkeit der entwickelnden Methoden sowie des dafür notwendigen zeitlichen Aufwands zu überprüfen. Entsprechende Adaptierungen fanden im Modell ihren Niederschlag. Dieser Entwicklungsschritt sollte mehrfach mithilfe nationaler und internationaler Experten durchlaufen werden, um die Grundlagen für eine taugliche KI-gestützte Analyse zu schaffen.

Auch wenn der Fokus beim Projekt auf hybride Einflussmöglichkeiten durch zukünftige Technologien lag, kann das erarbeitete Meta-Modell um weitere kombinierte Varianten hybrider Machtprojektionen erweitert bzw. geschärft werden.

Im Rahmen einer Anwendung innerhalb eines EU-Mitgliedsstaates, der mit divergierenden Bedrohungsperzeptionen konfrontiert ist, muss das Analysemodell zwangsweise an das Verhältnis dieses Staates adaptiert werden. Das triff sowohl auf die Operationalisierung der Akteure wie auch auf die Anpassung der Handlungsfelder zu. Dabei sind auch Anknüpfungspunkte zu den im Kontext der EU und NATO vorgeschlagenen Modelle zu berücksichtigen, wie im Ausblick ansatzweise beschrieben. Das zentrale Ziel des Meta-Modells HTM3 ist es die Grundlage für eine objektive Betrachtungsweise für alle beteiligten Staaten zu schaffen. Dabei kommen innovative Technologien, Methoden und Tools zum Einsatz.

Der Anspruch dieser Publikation ist es, einen Einblick in die Arbeit der Forschergruppe zu geben.

1.2. Projektbeschreibung

Der Zweck des Meta-Modells ist, mögliche sicherheitspolitische Auswirkungen aufzuzeigen, um rechtzeitig zur gesamtstaatlichen Resilienzsteigerung beizutragen. Diese Form der Frühwarnfunktion besitzt das Potential, auch einen Beitrag zum Analyseverfahren für das europäische Risikobild zu leisten.

Im ersten Prozessschritt der Bedrohungsanalyse wird eine Mischform menschlichen Expertenwissens und maschineller Verfahren verlinkt und folglich das Ergebnis von Experten überprüft. Die Resultate werden wiede-

rum in den Prozess eingespeist, um später Variablen für die KI zur Verfügung zu stellen, um möglichst autonom Trends zu erkennen. Gerade dieser erste Prozessschritt stellte das Projektteam vor Herausforderungen, da die komplizierte Kombination von Inputs der Experten, maschineller Beobachtung und der durch den Programmierer herzustellenden Verknüpfung besondere Kreativität erfordert[12].

Zu Beginn des Projekts standen folgende Forschungsfragen:

- Wie könnte ein Meta-Modell zur Analyse von Risiko- und Bedrohungspotentialen durch missbräuchliche Anwendung von neuen Technologien aussehen?
- Sind mit Hilfe eines derartigen Meta-Modells Risiko- und Bedrohungspotentiale überhaupt erkennbar?
- Kann dadurch die Resilienz und damit die Handlungsfähigkeit des Staates als Akteur erhöht werden?
- Wie lassen sich technologische Möglichkeiten identifizieren, um deren Zweckentfremdung zu Machtzwecken zu erkennen?

1.3. Struktur und Übersicht

Die Publikation gliedert sich wie folgt:

Die Einleitung erfolgt in Kapitel 1 und umfasst neben der Problemstellung sowie den Forschungsfragen die Projektbeschreibung.

Das HTM3 META-Model wird in Kapitel 2 anschaulich vorgestellt.

Im Rahmen des Projektes wurde das HTM3 META-Modell mit einer Pilotanwendung mehrfach getestet und durch Experten aus nationalen Behörden

[12] vgl. Alexander Armbruster, Kausalität. Was Künstlicher Intelligenz noch fehlt. Und warum sie dennoch längst nicht nur kommerziellen Erfolg von Misserfolg trennt, sondern auch politisch zu einer zentralen Macht-Variablen geworden ist. Frankfurter Allgemeine Zeitung, Montag, 10. Jänner 2022, Nr. 7, S. 21

evaluiert. Die Pilotanwendung und Evaluierung werden in Kapitel 3 dargestellt.
In Kapitel 4 findet sich die Zusammenfassung sowie die Ergebnisse des gegenständlichen Projektes.
Das Kapitel 5 beschreibt die internationalen Anknüpfungspunkte zu Modellen, die im Kontext von NATO und EU im Hinblick auf Hybride Bedrohungen vorgestellt wurden und geht auf mögliche Schnittstellen zu HTM3 ein, die in der operativen Umsetzung beachtet werden sollten. Des Weiteren werden hier auch technologische Entwicklungen und deren zukünftige Einflüsse auf das Modell dargestellt. Der Ausblick, bzw. Ableitungen und Folgerungen aus den bisherigen Forschungsergebnissen werden in Bezug auf die Varianten der operativen Umsetzung im Ausblick beschrieben.

2. HTM3 META-Modell

Das Meta-Modell für Horizon Scanning und kollaborative Wissensentwicklung zur systematisierten Erfassung, Strukturierung und Visualisierung hybrider Bedrohungen im Kontext unkonventioneller Kriegsführung versucht erstmalig aufzuzeigen, wie aus einem unstrukturierten Informationsraum eine strukturierte Datenerfassung abgeleitet werden kann, die frühzeitig gesamtstaatliche strategische Handlungsoptionen ermöglichen soll. Die besondere Herausforderung dabei ist, dass per Definitionem die Ereignisse, die Themen, die Akteure und der Kontext unlimitiert und nicht vorhersehbar sind.

Das European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) definiert:

- "Coordinated and synchronized action that deliberately targets democratic states´ and institutions´ systemic vulnerabilities through a wide range of means.
- Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international).
- Activities aimed at influencing different forms of decision-making at the local (regional), state or institutional level and designed to further and/or fulfil the agent´s strategic goals while undermining and/or hurting the target."[13]

Diese Definition greift jedoch zu kurz, wenn es um unkonventionelle Kriegsführung geht. Schon alleine an der Vielzahl der Bezeichnungen zeigt sich,

[13] Georgios Giannopoulos, The Landscape of Hybrid Threats: A Conceptual Model, Public Version, Luxembourg: Publications Office of the European Union, 2021, European Union and Hybrid CoE, 20212021, ISBN 978-92-76-29819-9, ISSN 1831-9424, doi:10.2760/44985, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC123305/conceptual_framework-reference-version-shortened-good_cover_-_publication_office_1.pdf

dass sich ein fundamentaler Strukturwandel in der Strategie und Taktik der Kriegsführung anbahnt, der vor allem auch durch Innovationsmanagement adressiert werden kann. [14] Das Hybrid CoE führt folgende Begriffe im Kontext unkonventioneller Kriegsführung an:
"surrogate warfare", "grey zone activity", "raiding", "unrestricted warfare" (origins Chinese), "reflexive control" (origins Russian), "new generation warfare"(origins Russian), "competition short of conflict", "active measures" (origins Russian), "non-linear warfare", "asymmetric warfare", "compound warfare" "ambiguous warfare", "political warfare", "information warfare", "cyber warfare".[15] Nicht alle Begriffe beschreiben das Gleiche, aber alle zählen in der einen oder anderen Form zur unkonventionellen Kriegsführung und somit zu hybriden Bedrohungen.

Das Konzept der unkonventionellen Kriegsführung ist nicht neu. In dem allgemeinen Sinne ist es der älteste, aber auch immer noch erfolgreichste Entwurf, einen Kampf durch den Einsatz von Fähigkeiten zu gewinnen, die für den Gegner neu und unerwartet sind. Die Art wie Krieg geführt wird, ist eine hochinnovative Aktivität, bei der die Suche nach „neuen Strategien" zur Vorbereitung eines jeden Konflikts gehört. Große gesellschaftliche Umbrüche, wie die Erfindung der Eisenverarbeitung, aber auch die Digitalisierung, führten auch immer zu Innovationen in der Strategie und Taktik der Kriegsführung. Selbst die Entwicklung des Computers hatte und hat stets einen enormen Einfluss auf Strategien, Fähigkeiten und Optionen, einen Krieg zu

[14] Volodymyr Zahorskyi, Andriy Lipentsev, Svitlana Andreyeva, Peculiarities of Public Administration Development in Ukraine in the Conditions of Democratic Transition: Status and Instruments VISION 2020: SUSTAINABLE ECONOMIC DEVELOPMENT AND APPLICATION OF INNOVATION MANAGEMENT, 2018

[15] Georgios Giannopoulos, The Landscape of Hybrid Threats: A Conceptual Model, Public Version, Luxembourg: Publications Office of the European Union, 2021, European Union and Hybrid CoE, 20212021, ISBN 978-92-76-29819-9, ISSN 1831-9424, doi:10.2760/44985, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC123305/conceptual_framework-reference-version-shortened-good_cover_-_publication_office_1.pdf

gewinnen. Doch wir stehen erst am Anfang dieses Strukturwandels. Daher vermitteln neue Konzepte für unkonventionelle oder hybride Kriegsführung, so wie es in Russland bezeichnet wird[16], nur einen ersten Eindruck möglicher Innovationen. Das chinesische Konzept des Unrestricted Warfare[17] zeigt, dass die Auflösung von Grenzen im konzeptuellen Denken auch die militärische Taktik verändert. Damit sind allerdings die konkreten neuen Möglichkeiten noch nicht beschrieben. Der „Fourth-Generation Warfare" (4GW)[18] oder der „Holistic Warfare"[19], wie er von den USA und den Staaten der EU beschrieben wird, zeigt auf, dass unter den neuen Möglichkeiten vor allem Cyberfähigkeiten verstanden werden, die sich aktuell gerade erst herausbilden. Das operative Umfeld besteht dabei aus den klassischen militärischen Domains, Land, Luft und Wasser, sowie den neueren Domains Weltraum und Cyber. Der Cyber Raum stellt dabei eine Art Meta Domain dar, die alle anderen Domains durchdringt und die alle soziokulturellen Faktoren über den Wissensraum mit dem Bereich der haptischen Welt verbindet. Diese abstrakte Beschreibung hat durchaus dramatische reale Implikationen für zukünftige strategische und taktische Planungen von militärischen Operationen.

[16] Christoph Bilban, Hanna Grininger (Hrsg.), Mythos "Gerasimov-Doktrin" Ansichten des russischen Militärs oder Grundlage hybrider Kriegsführung?, Schriftenreihe der Landesverteidigungsakademie, Band 2/2019

[17] Qiao Liang, Wang Xiangsui, Unrestricted Warfare, PLA Literature and Arts, Publishing House, February 1999

[18] William S. Lind, Gregory A. Thiele, 4th Generation Warfare, 2016, https://archive.org/details/4th-generation-warfare-handbook

[19] Sean Kimmons, Army strategizing for holistic change, not just new tech, 2017

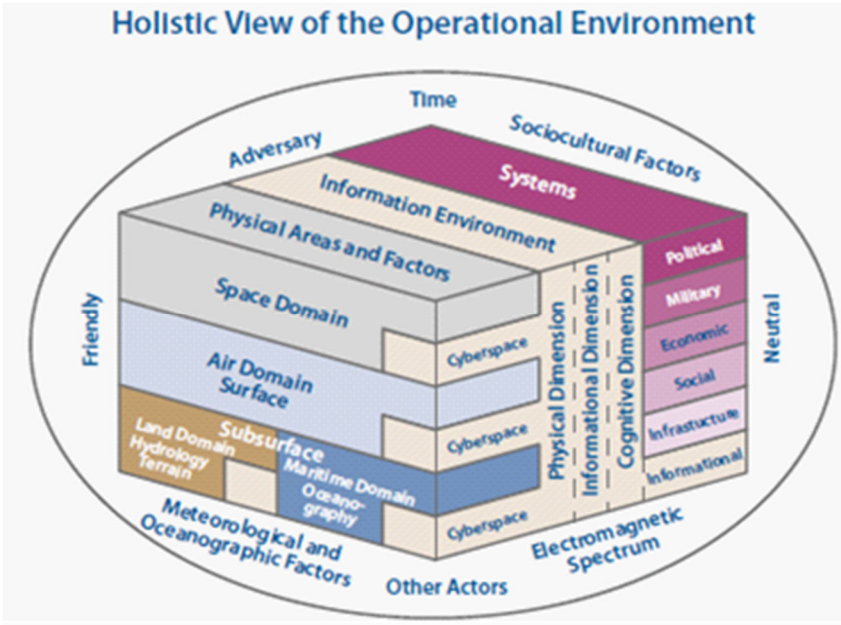


Abbildung 2 – Holistic View of the Operational Environment[20]

Indem die Cyber Domain den Informations- und Wissensraum prägt, verbindet sie alle soziokulturellen Faktoren mit den militärischen Domains und bietet damit den zentralen Punkt für eine gezielte Einflussnahme auf das Kriegsgeschehen. Die holistische Perspektive auf das Einsatzgebiet verringert einen eingeschränkten Blick, erlaubt aber noch nicht eine strategische oder taktische Konzeption.

Das Metamodell für Horizon Scanning und kollaborative Wissensentwicklung (HTM3) wurde zeitgleich und unabhängig vom „Framework for Cross-

[20] The Joint Air Power Competence Centre, Joint Air & Space Power Conference. Shaping NATO for Multi-Domain Operations or the Future, 2019, Germany, S. 9, https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf

Domain Strategies Against Hybrid Threats“[21] entwickelt, allerdings nach Erscheinen des Framework for Cross-Domain Strategies Against Hybrid Threats soweit abgeglichen, dass Anknüpfungspunkte für eine parallele Verwendung identifiziert wurden, die im Ausblick zur operativen Verwendung beschrieben werden. Dabei sind Unterschiede zutage getreten, die sich aus der Motivation der Modellentwicklung ergeben. HTM3 wurde entwickelt, um eine Infrastruktur zu schaffen, die, ausgehend von realen Events hybrider Bedrohung, die kollaborative Wissensentwicklung automatisiert und durch Horizon Scanning beschleunigt. Dabei wurde ein bottom-up Ansatz verwendet. TNO Framework verfolgt mit der Kategorie Bildung einen Top-down Ansatz, der durch den bottom-up Ansatz von HTM3 ergänzt werden könnte. HTM3 sieht einen Prozess der kontinuierlichen Verbesserungen aufgrund empirischer Erfahrungen vor, bei dem die Taktiken aus den jeweils identifizierten Ereignissen hybrider Bedrohung extrahiert und dokumentiert werden.

Durch Horizon Scanning lassen sich mit dem HTM3 Modell alle Komponenten eines klassischen Horizon Scanning zu Hybriden Bedrohungen, wie z.B. im Report von TNO[22] updaten. Dazu braucht es zum einen, die vorbereitende Modellierung, die richtigen Crawler und die analytischen Komponenten, um die relevanten Daten zu extrahieren. Weiters wurde HTM3 entwickelt, um die Prozesse für ein KI gestütztes Horizon Scanning zu optimieren.

[21] Tim Sweijs, Samuel Zilincik, Frank Bekkers, Rick Meessen, Framework for Cross-Domain Strategies Against Hybrid Threats, 2021, https://euhybnet.eu/wp-content/uploads/2021/06/Framework-for-Cross-Domain-Strategies-against-Hybrid-Threats.pdf

[22] Rick Meessen, et. all., A HORIZON SCAN OF TRENDS AND DEVELOPMENTS IN HYBRID CONFLICTS SET TO SHAPE 2020 AND BEYOND, 2021, https://euhybnet.eu/wp-content/uploads/2021/06/TNO-HCSS-Horizon-scan-Hybrid-Trends-and-Developments-2002-.pdf

Vor Projektbeginn standen für die Idee und Methode der Meta-Modell Erstellung, welche gemeinsam mit allen Projektbeteiligten erstellt wurde, drei Fragen im Vordergrund. Die Beantwortung dieser Fragen ist Voraussetzungen zur Erreichung der Projektziele und lauten wie folgt:

- Kann durch bereits gewonnene Erkenntnisse und Erfahrungen im Bereich der Modellierung und mit Unterstützung von „Mustermodellen“ und operativen Modellen ein wesentlicher Mehrwert für dieses Projekt generiert werden? Insbesondere der Wunsch nach einem Meta-Modell wäre hier anzustreben.
- Kann durch die vorhandenen OSInfo-Datenbestände und eine rasch anpassbare Modellerweiterung wesentlich zum Wissensgewinn für alle am Projekt beteiligten Akteure beigetragen werden – insbesondere auch durch die Implementierung eines sogenannten „Horizon Scanning Center“?
- Kann durch bereits erprobte und weiter zu entwickelnden Mechanismen einer zeitgemäßen Wissensentwicklung eine Qualitätssteigerung erreicht werden? Sind modernste Verfahren der Analyse, des „Maschinellen Lernens“ oder der Einsatz von „Künstlicher Intelligenz“ nachvollziehbar und sinnvoll einsetzbar?

Die Vorgangsweise zur Beantwortung dieser drei Fragestellungen fußte in der Entwicklung des „Hybride Bedrohungen – Technologie“ Meta-Modelles HTM3, welches in diesem Kapitel vorgestellt wird. Die nachfolgende Graphik gibt eine Übersicht über das Meta-Modell. Die Bezeichnung „Meta“ Modell wurde deshalb gewählt, weil in jedem einzelnen Prozessschritt eine Vielzahl an unterschiedlichen Modellen zum Einsatz kommen und das Meta-Modell den Rahmen für die Prozessschritte in den folgenden 6 Modulen bildet:

- **Wissensraum**: Das Modul definiert alle Services, die zur Erfassung Strukturierung und Analyse des Wissensraumes notwendig sind. Bei hybriden Bedrohungen ist dieser Wissensraum typischerweise deutlich breiter gefächert als bei klassischen wissenschaftlichen Studien. Neben Publikationen umfasst der Wissensraum eine Vielzahl unterschiedlicher Quellen aus dem Surface Web, dem „deep net" und dem „dark net".

- **Akteure und Handlungsfelder aus globaler Perspektive**: In diesem Modul werden die Akteure aus einer globalen Perspektive dargestellt und analysiert, soweit dieses theoretisch zu erschließen ist. Das Modul bereitet damit die operative Akteursanalyse vor, die in Kapitel 4.1 beispielhaft umgesetzt wurde.

- **Use Case Bearbeitung:** In diesem Modul werden die Prozesse der operativen Umsetzung definiert und beispielhaft für einen Erstbetrieb bearbeitet. Dabei wurde ein neues Konzept angewandt, um synchronisiert und transparent Expertenwissen zu erfassen und zu dokumentieren.

- **Wirkungsbereich Staat**: Dieses Modul definiert die Prozesse der operativen Analyse. Der Staat wird dabei als Treiber einer Wirkung gesehen, für deren Analyse die entsprechenden korrespondierenden Prozesse definiert werden. Um der hohen Innovationsgeschwindigkeit hybrider Bedrohungen gerecht zu werden, müssen die Prozesse so definiert sein, dass diese mit einem potentiell unbegrenzten Wirkungsbereich eines Staates umgehen können.

- **Unterstützende Services**: Hier werden alle Prozesse für unterstützende Services zusammengefasst, die noch nicht in anderen Modulen behandelt wurden. Unterstützende Services sind z.B. Recherche

Tätigkeiten, Informationszusammenstellungen oder programmierte Datenbeschaffungsinstrumente.

- **Organisationsentwicklung und Transformation**: In dem entsprechenden Modul werden die Prozesse zusammengefasst, die zur Transformation und Organisationsentwicklung beitragen. Das können sowohl einzelne Stakeholder Workshops als auch ganze strukturverändernde Aktivitäten sein.

Die folgende Abbildung bietet einen Überblick über das Meta Modell HTM3. Da dieses in der hier verwendeten verkleinerten Auflösung nur zum Teil lesbar ist, wurde im Anhang eine Graphik in einem vergrößerten Format hinzugefügt. Zusätzlich sind die graphischen Darstellungen der einzelnen Module jeweils im Kapitel der Modulvorstellung vergrößert dargestellt.

Meta-Modell:

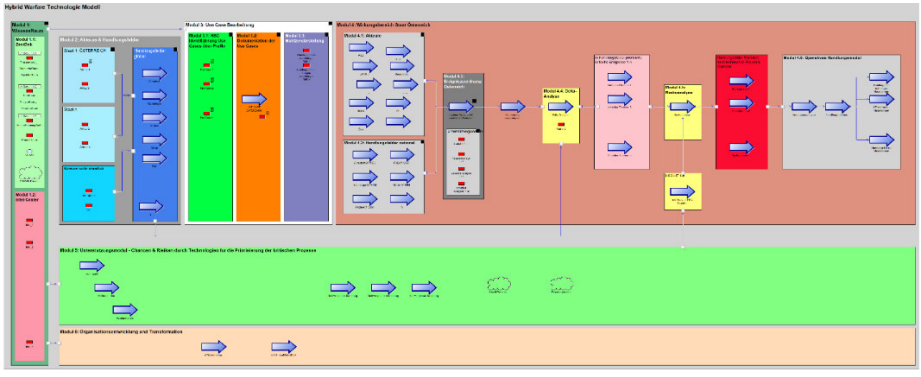


Abbildung 3 – „Hybride Bedrohungen – Technologie Meta-Modell“

Das Erstellen des Meta-Modelles durch das Projektteam erfolgte in zyklischen Schritten und wurde so konzipiert, dass iterative Verbesserungen im Betrieb nicht zu inkonsistenten Datensätzen führen. Diese Offenheit und

Flexibilität gegenüber neuen Entwicklungen und innovativen hybriden Bedrohungen ist notwendig, um auf die große Innovationskraft und hohe Innovationsgeschwindigkeit von hybriden Operationen reagieren zu können.

Die Bezeichnung „Meta“ Modell wurde deswegen gewählt, weil in jedem einzelnen Prozessschritt jeweils wieder eine Vielzahl an unterschiedlichen Modellen zum Einsatz kommen und das Meta-Modell gewissermaßen den Rahmen bildet für die Prozessschritte in den entsprechenden Modulen.

Die Module selbst sind Cluster an Prozessen, die jeweils so konzipiert sind, dass die Module interoperabel sind und gegen andere Module ausgetauscht werden können. Im Folgenden werden die Module im Einzelnen beschrieben.

Modul 1 „Wissensraum“:

Im Modul 1 befindet der sog. „Wissensraum“. Dieser besteht aus zwei wesentlichen Komponenten: Einerseits aus Elementen der ZentDok, andererseits dem „Intel-Center“. Für diese Publikation wird nur Ersteres im Detail beschrieben. Operative Intel-Elemente werden bei Bedarf für konkrete Umsetzungsmaßnahmen eingebunden.

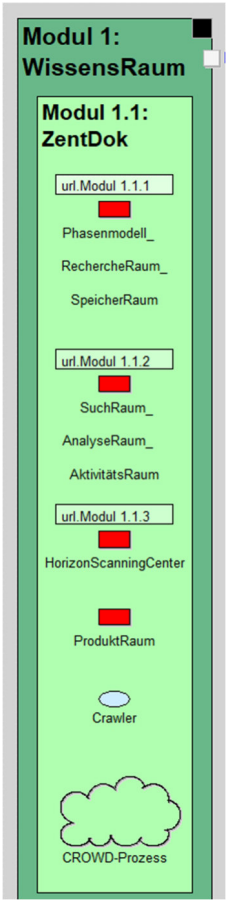


Abbildung 4 – Modul 1: „Wissensraum“ – Auszug Modul 1.1 ZentDok

Modul 1.1 „ZentDok“:

Im Anwendungsfall werden drei wesentliche Elemente der ZentDok eingebunden, die für alle Projektschritte abruf- und anpassbar sind. Der Rechercheraum (1.1.1), der in verschiedensten Kombinationen zur Verfügung stehende Such- und Analyseraum (1.1.2) sowie das „Horizon Scanning Center“

(„HSC“) (1.1.3). Insbesondere das „HSC“ ermöglicht eine spezielle Anpassung an die Erfordernisse des Informations- und Wissensbedarfes für die ins Projekt eingebundenen Experten.
Hintergrund dieser Konzeptionen sind die sog. „Fragen-“ und die „Assoziationsheuristik“, welche die Grundlage des ZentDok „Phasenmodells“ darstellen.[23] Ebenso werden verschiedene Analyseschritte aus der in Verwendung stehenden Analysetools der ZentDok berücksichtigt. Diese umfassen Terminologie Analyse Tools wie „ProTerm“ oder den Einsatz von IBM Watson und IBM – i2.[24]
Alle oben angeführten Produkte des „Produktraumes“ der ZentDok stehen dem Projekt ebenso zur Verfügung, wie verschiedenste Crawlerfunktionalitäten oder Recherchetätigkeiten der sog. „Cyber-Rekruten“ des CDFZ („Cyber Dokumentations- und Forschungs-Zentrum“) der ZentDok.
Diese Möglichkeiten werden durch sog. CROWD-Prozesse unterstützt, um relativ rasch auf neue Anforderungen im Projektverlauf reagieren zu können.

Modul 1.1.1 „Recherche Raum“

Im nachfolgenden „Phasenmodell Recherche Raum Meta“ der ZentDok werden alle Open Source Daten und deren zeitlich und inhaltlich zusammenhängende Logik dargestellt und beschrieben. Dieses Modell kann für verschiedenste Anwendungsfälle adaptiert werden – daher die Bezeichnung „Meta“.

---

[23] Klaus Mak, Joachim Klerx, Hans Christian Pilles, Johannes Göllner, Wissensentwicklung mit „Crows OSInfo“, Eine Innovation des Cyber Documentation & Research Center (CDRC) der Zentraldokumentation (ZentDok), Landesverteidigungsakademie (LVAk), Schriftenreihe der Landesverteidigungsakademie, 2015

[24] Klaus Mak, Hans Christian Pilles, Markus Bertl, Joachim Klerx, Wissensentwicklung mit IBM Watson in der Zentraldokumentation (ZentDok) der Landesverteidigungsakademie, Entwicklungen und Anwendungen in der Open-Source Informationsbereitstellung des ÖBH, Schriftenreihe der Landesverteidigungsakademie, 2018

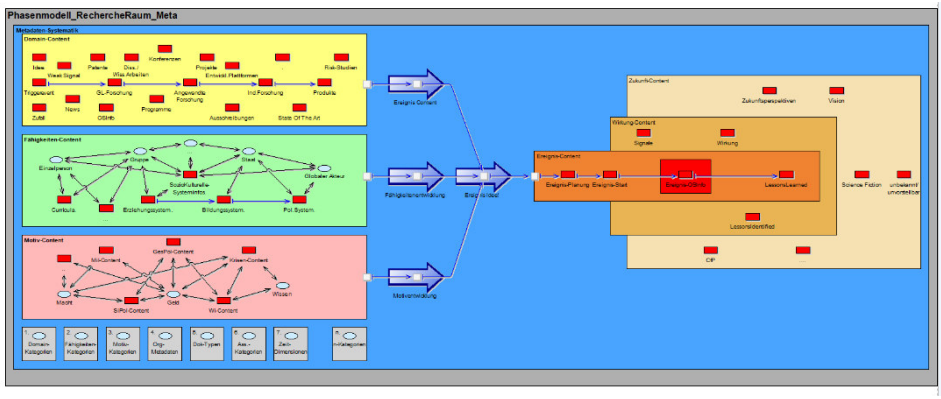


Abbildung 5 – Phasenmodell Recherche Raum Meta[25]

Es werden folgende Bereiche unterschieden:

- „Domain-spezifischer Content“,
- „Fähigkeiten-spezifischer Content“,
- „Motiv-spezifischer Content“ sowie eine umfassende
- „Metadaten-Systematik“.

Alle Produktinhalte werden in Form eines „Phasenmodells“ zeitlich angeordnet, um so auch eine Zuordnung über den Erstellungshorizont einzelner spezifischer Ereignisse analysieren zu können. Über die Dokumententypisierung lässt sich diese heuristische Modellierung technisch bzw. maschinell auswerten.

Über ein tägliches Update werden alle Dokumente - ausgestattet mit Metadaten und zusätzlichen Assoziationskriterien - tagesaktuell für Recherchen und Analysen allen Projektbeteiligten bereitgestellt.

[25] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

Modul 1.1.2 „Analyse Raum“

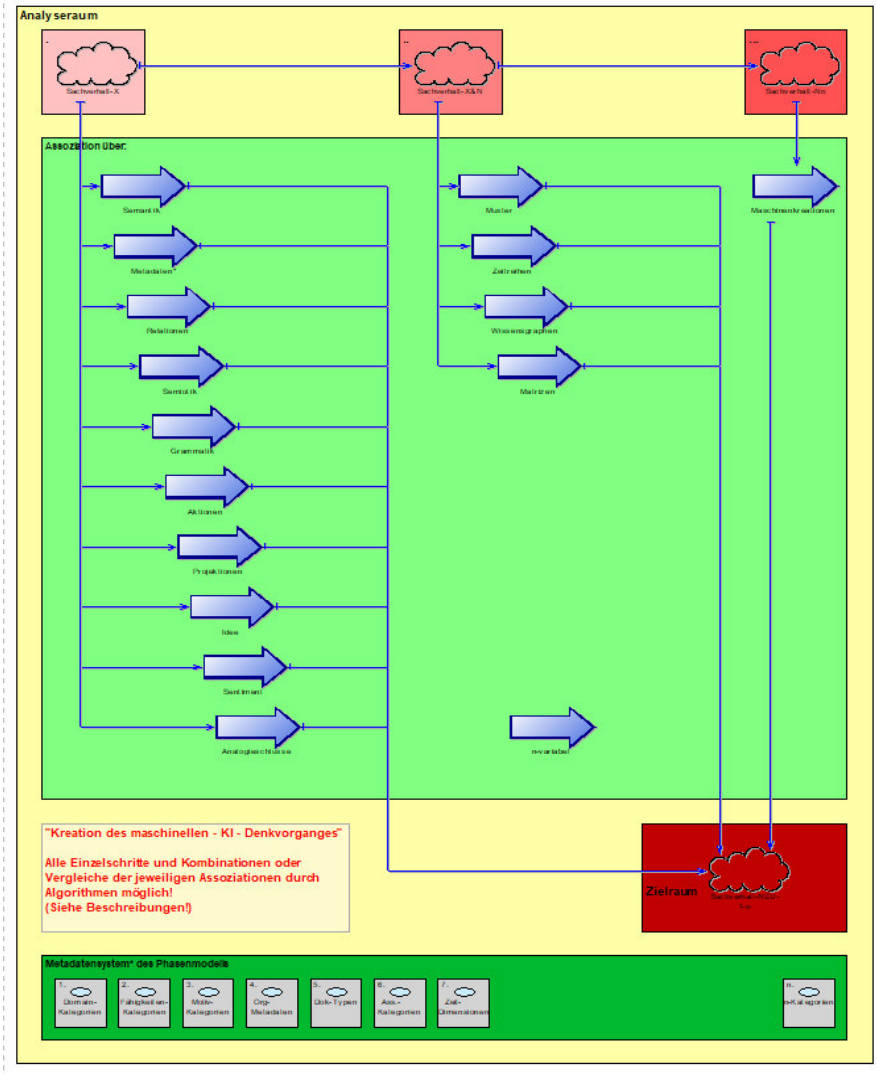


Abbildung 6 – Analyse Raum[26]

[26] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

Die Möglichkeit, alle Inhalte aus dem „Recherche Raum“ nicht nur für Suchanfragen ständig zur Verfügung zu stellen, sondern auch mithilfe aller maschinellen Möglichkeiten analysieren zu können, wird über eine systematische Erfassung aller bestehenden Variationen, methodisch strukturiert erfasst.
Im Analyse Raum werden alle relevanten Sachverhalte durch Assoziationen oder Assoziationsbündel zu neuen Sachverhalten kreiert. Der „maschinell unterstützte Lernvorgang“ ermöglicht eine Basis für eine bisher nicht umsetzbare Kreation von unbekannten und neuen Sachverhalten.
Assoziationen erfolgen über das Erkennen von „sinnvollen“ Zusammenhängen (bspw.: semantisch, semiotische, grammatikalische) oder Mustererkennung, Zeitreihen, anderer Algorithmen des sog. „Maschinellen Lernens“ oder der „Künstlichen Intelligenz“.
Alle Metadatenvariationen des Phasenmodells und qualitätsgesicherte Inhalte, mit verschiedensten Typisierungsmerkmalen, können so zu den jeweiligen relevanten neuen Sachverhalten im „Zielraum“ den Experten zur Verfügung gestellt werden.

Modul 1.1.3 „Horizon Scanning Center“

Durch die Implementierung eines sog. „Horizon Scanning Centers“ (HSC) werden allen am Projekt beteiligten Personen über Profildienste Fachinformationen zur Verfügung gestellt.

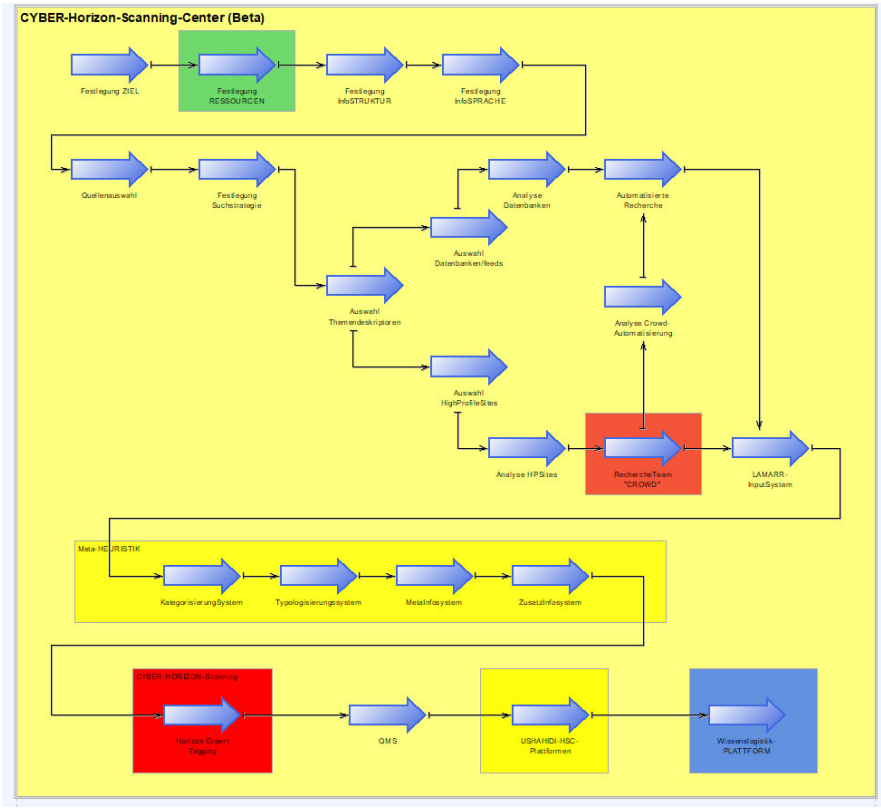


Abbildung 7 – „Horizon Scanning Center“ – Beta-Version[27]

Diese Informationsbereitstellung erfolgt nach Abstimmung mit allen Nutzern und kann variabel konfiguriert werden. Über sog. „Push- oder Pull-Dienste“ können die gescannten Inhalte des jeweiligen „Interessenshorizont“ der Nutzer in zeitlich steuerbaren Perioden zur Verfügung gestellt werden.

[27] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

Modul 2 „Akteure & Handlungsfelder“ (globale Sichtweise)

Im Modul 2 (Abbildung 8) werden alle relevanten Akteure identifiziert. Diese Akteure werden grundsätzlich unterschieden zwischen staatlichen und nicht staatlichen Akteuren. Weiters erfolgt in diesem Modul auch die Identifikation der globalen Handlungsfelder.

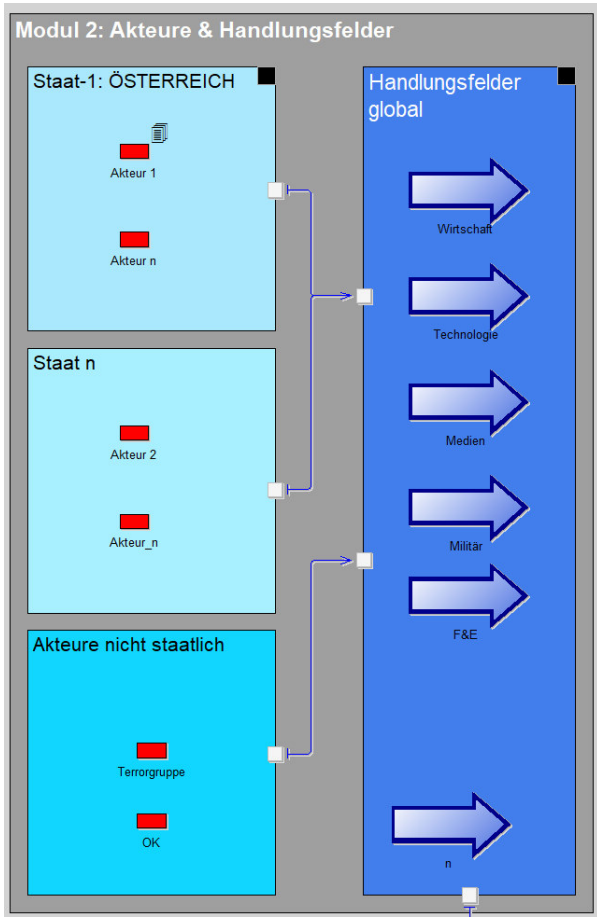


Abbildung 8 – Akteure und Handlungsfelder[28]

[28] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

Modul 3 „Use Case Bearbeitung“

In diesem Modul (Abbildung 9) erfolgen die Extraktion und Formalisierung des verfügbaren Expertenwissens. Die Bearbeitung der Use Cases wurde durch mehrere Personenkreise getestet, um die Methode der Erhebung (Strukturierung, Metadaten, etc.) zu evaluieren.

Durch den in Kapitel 1.1 angeführten interministeriellen sowie aus internen und externen Personen bestehenden Expertenpool wurde in mehreren Iterationen die Testung durchgeführt und bereits erste Inhalte bereitgestellt.

Die Use Cases wurden aus dem unmittelbaren Arbeitskontext durch die Experten ausgewählt und beschrieben. Dieser Personenkreis evaluierte und adaptierte auch die vorerst erkannten Handlungsfelder.

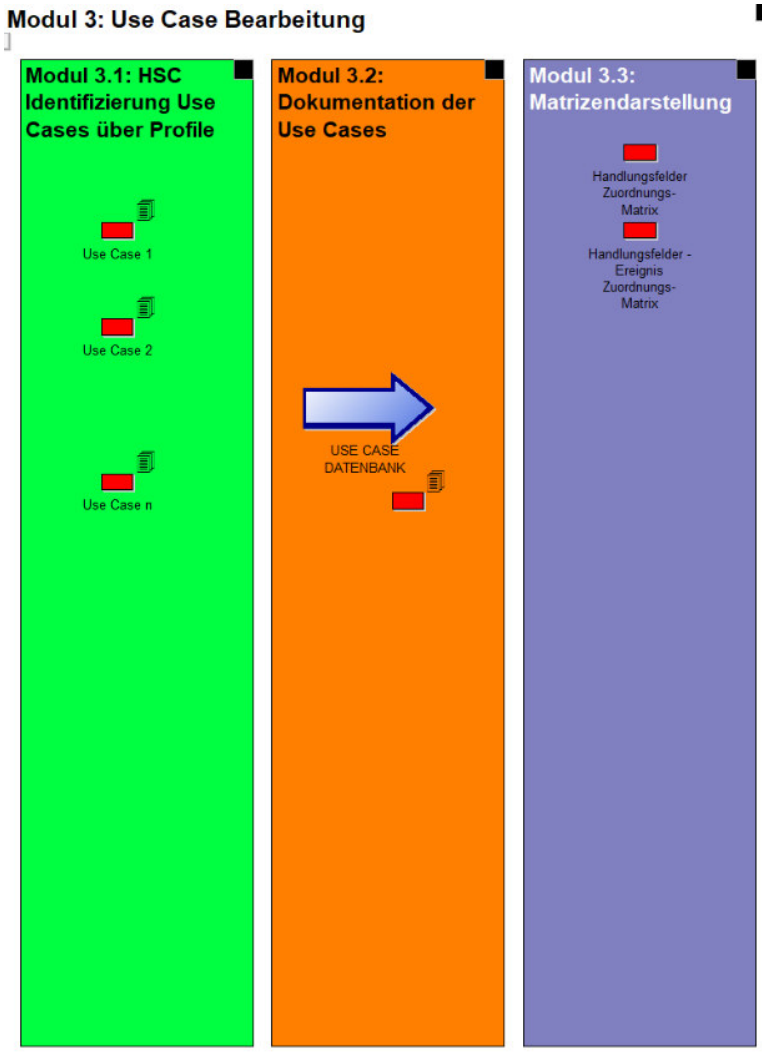


Abbildung 9 – Use Case Bearbeitung - Auszug[29]

In weiterer Folge kann der Personenkreis qualitativ und quantitativ erweitert werden und an die jeweiligen Anforderungen flexibel angepasst werden.

[29] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

Modul 3.1 "HSC Identifizierung Use Cases über Profile"

Die Use Cases wurden beispielhaft, basierend auf vorhandenem Expertenwissen sowie über die zur Verfügung gestellten Profildienste (Abbildung 7), ausgewählt und priorisiert den identifizierten Handlungsfeldern zugeordnet. In dieser Kategorie werden durch die jeweiligen Experten alle für den spezifischen Kontext relevanten Use Cases identifiziert und beschrieben.

Modul 3.2 "Dokumentation der Use Cases"

Mit einer intern programmierten Datenbank werden alle Informationen zu den identifizierten Use Cases zur weiteren Bearbeitung gespeichert. Die Struktur richtet sich nach einem iterativ entwickelten excelbasierten Erfassungs- bzw. Erhebungsbogen. Durch diese Erfassungssystematik wird verfügbares Expertenwissen tiefgreifend strukturiert erfasst und stellt somit die Grundlage für zusätzliche Maschine Learning- und/oder KI-Anwendungen dar.

Dieses Erfassen des Expertenwissens stellt den Kern des gegenständlichen Projektes dar. Durch diese Expertise in allen zu identifizierenden und zu bearbeitenden Use Cases kann eine entsprechende Qualität sichergestellt werden und ermöglicht weitere Analysetätigkeiten.

Modul 3.3 "Matrizendarstellung"

Dieses Modul beinhaltet die Darstellung sämtlicher Informationen in verschiedensten zweidimensionalen Matrizen. Diese stellen die Grundlage für die allgemeinen wie spezifischen weiteren Analysen dar.

Die Gesamtheit aller erfassten Meta-Daten und Content-Entitäten dienen als Basis für mögliche projektrelevante Matrizen. Unterschiedliche Matrizen erlauben kurz-, mittel- und/oder langfristige Analysen zur Identifikation themenübergreifender Zusammenhänge. Durch die Anordnung verschiedener Matrizenlayer entsteht eine mehrdimensionale Betrachtungsmöglichkeit der Analyseergebnisse für den nächsten Schritt. Staatliche und nichtstaatliche Experten begleiten diese Phase im nachfolgenden Modul 4.

In der ZentDok steht neben den technischen Tools ebenso das erforderliche Wissen über deren Anwendung zur Verfügung. Bei den Analysen für das gegenständliche Projekt kommen insbesondere statistische Methoden wie etwa Netzwerkanalysen zum Einsatz.

Modul 4 „Wirkbereich Staat Österreich“

In diesem Modul sind die Anwendungen des Modells exemplarisch für den „Staat Österreich“ als mögliches Zielland einer hybriden Bedrohung modelliert.

Das Modul 4 „Wirkbereich Staat Österreich“ setzt sich aus mehreren, in weiterer Folge näher beschriebenen Submodulen zusammen. Diese stellen sich wie folgt dar:

- Modul 4.1 Akteure
- Modul 4.2 Handlungsfelder (national)
- Modul 4.3 Ereigniszuordnung Österreich
- Modul 4.4 Delta-Analyse
- Modul 4.5 Risikoanalyse
- Modul 4.6 Operatives Handlungsmodul

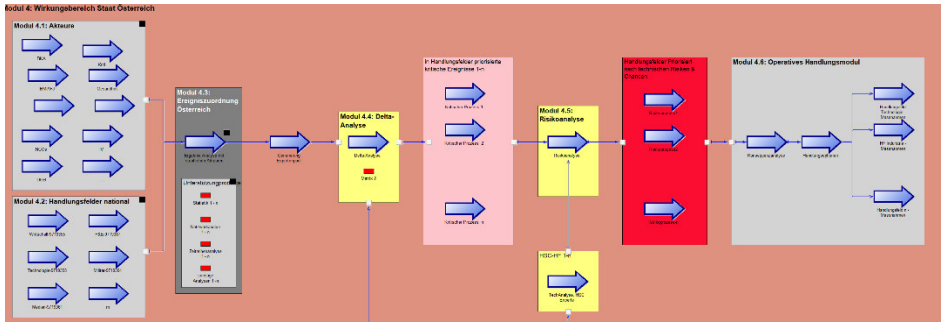


Abbildung 10 – Wirkbereich Staat Österreich[30]

Eine vergrößerte Ansicht der obigen Abbildung 10 befindet sich im Anhang.

[30] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

Modul 4.1 „Akteure“

Dieses Modul besteht aus sämtlichen staatlichen als auch nichtstaatlichen Akteuren des Wirkbereiches.

In der Abbildung sind einige dieser Akteure für den Wirkbereich Österreich exemplarisch aufgelistet. Selbstverständlich sind diese Akteure für andere Wirkbereiche (bspw. andere Staaten) spezifisch zu identifizieren.

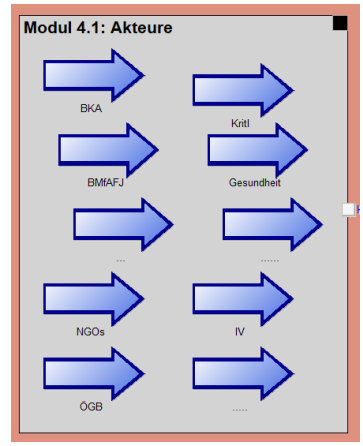


Abbildung 11 – Modul 4.1: Akteure (Auszug aus Modul 4)[31]

Modul 4.2 „Handlungsfelder national“

Sind jene Handlungsfelder welche durch den oben angeführten Personenkreis als für den Staat relevante Handlungsfelder festgelegt wurden.

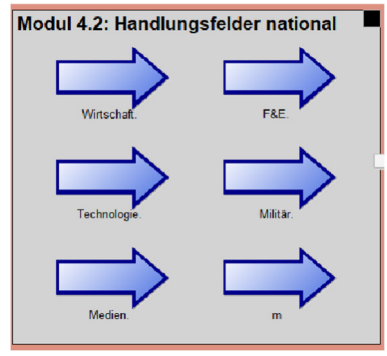


Abbildung 12 – Handlungsfelder national[32]

[31] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok
[32] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

Modul 4.3 „Ereigniszuordnung Österreich“

Von Domainexperten/Akteuren Staat Österreich über Beurteilung der Ergebnisse aus Unterstützungsprodukten mit dem Ergebnis der notwendigen Experten zu Ereignisanalyse im nächsten Schritt. (Expertenpool)

Staatl. Akteure sind verantwortlich für die Beurteilung der Ergebnisse aus Matrizen und anderen Expertisen aus der Datenbank zu den jeweiligen Ereignissen.

Unterstützungsprodukte (Auswahl):

Statistik 1 – n, Netzwerkanalyse 1 – n, Zeitreihenanalyse 1 – n, …

Diese Unterstützungsprodukte sind bspw. Netzwerkanalysen basierend auf den verfügbaren auswertbaren Matrizen sowie Wissen aus der Ereignisdatenbank und stellen neben der jeweilig vorhandenen Expertise eine Grundlage für die "Ergebnis Analyse mit staatlichen Akteuren" dar.

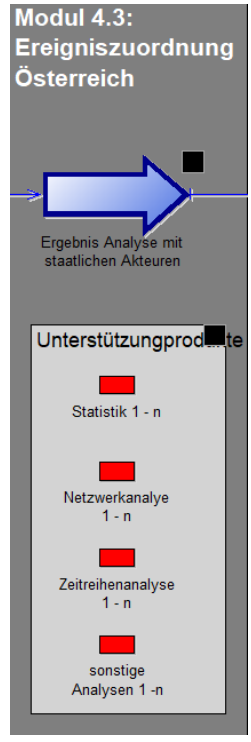


Abbildung 13 – Ereigniszuordnung Österreich[33]

Modul 4.4 „Delta-Analyse“

Mit dem generierten Expertenpool erfolgt in diesem Modulabschnitt eine Delta-Analyse (Abbildung 14) inwieweit globale Einflüsse auf die „Ereigniszuordnung Österreich“ (Abbildung 13) Einfluss nehmen.

Als Ergebnis wird eine Übersicht über alle relevanten Handlungsfelder mit den neu priorisierten Ereignissen und den dazu gehörenden kritischen Prozessen herausgearbeitet. Serviciert wird dieses Modul durch die relevanten Informationsinhalte bezogen auf die globalen Handlungsfelder aus Modul 2.

[33] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

Die globalen Handlungsfelder ermöglichen dabei in Verbindung mit dem staatlichen Layer (bspw. Österreich) eine zusätzliche Sichtweise zur Unterstützung der Priorisierung der kritischen Ereignisse und/oder Prozesse.

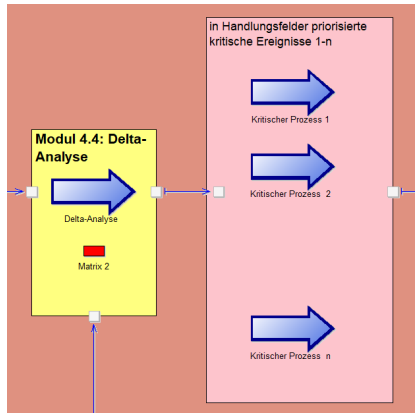


Abbildung 14 – Delta-Analyse samt Ablaufprozess[34]

Modul 4.5 „Risikoanalyse“

Gemeinsam mit dem „Tech-Analyse, HSC Experte“ – Gremium wird eine Risikoanalyse durchgeführt. Als Ergebnis werden Handlungsfelder priorisiert-nach technischen Risiken und auch Chancen festgelegt. Als Ergebnis sind konkrete Risikoprozesse zu definieren. In der nachfolgenden
In der Abbildung 15 ist das Modul 4.5 visualisiert.

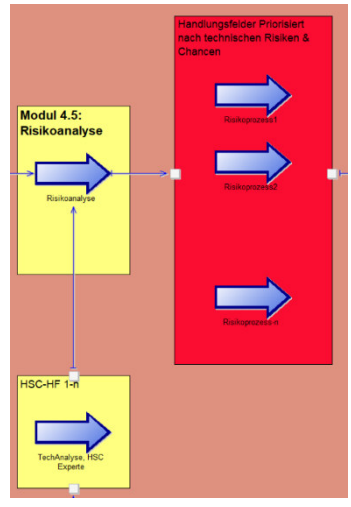


Abbildung 15 – Risikoanalyse[35]

[34] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok
[35] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

Modul 4.6 „Operatives Handlungsmodul“

In diesem Modul werden abschließend nach einer „Konsequenzanalyse“ und den daraus resultierenden Handlungsoptionen durch alle Akteure konkrete Maßnahmen in den jeweiligen Handlungsfeldern herausgearbeitet.

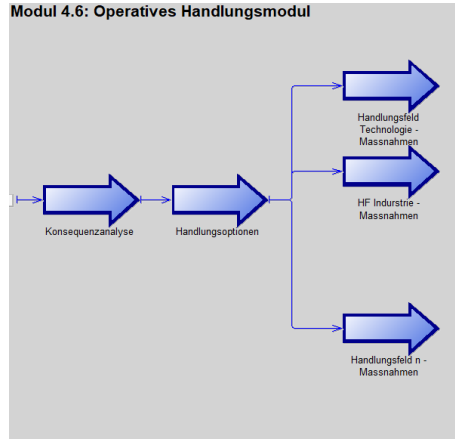


Abbildung 16 – Operatives Handlungsmodul[36]

Modul 5 „Unterstützungsmodul“

Um Chancen & Risiken durch neue Technologien für die Priorisierung der kritischen Prozesse erkennen zu können, kann über das HSC des Rechercheraumes jeder Technologie-Experte seinen Informationsraum abscannen. Damit können parallel zu anderen Modulprozessen jederzeit risikospezifische Ereignisse kurz-, mittel- und/oder langfristig dokumentiert werden. Unterstützt wird dies auch durch Crowd-Prozesse, die on demand abrufbar sind.

Daher sind die Grundlagen für die Delta-Analyse jederzeit aktuell abrufbar.

Abbildung 17 – Unterstützungsmodul[37]

[36] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok
[37] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

Modul 6 „Organisationsentwicklung und Transformation“

Dieses Modul stellt einen möglichen Bestandteil eines operativen Modelles für eine Organisation dar. Die Module 1 bis 6 repräsentieren in vielen Bereichen Grundlagen für eine Organisationsentwicklung sowie Transformationsprozesse. Das Wissens-Performance-System (WPS)[38] und die dazugehörige WM-Architektur ÖBH[39] kann als Grundlage für weitere Implementierungen in operativen Umsetzungen herangezogen werden.

[38] Vgl. Robert Woitsch, Klaus Mak, Johannes Göllner, Grundlagen zum Wissensmanagement im ÖBH. Teil 2: Wissensbilanz als Steuerungsinstrument im ÖBH: Ein Evaluierungs-Rahmenwerk aus der Sicht praktischer Anwendungen, Schriftenreihe der Landesverteidigungsakademie 10/2010, Wien, 2010

[39] Vgl. Johannes Göllner, Klaus Mak, Robert Woitsch, Grundlagen zum Wissensmanagement im ÖBH. Teil 1: Ein WM-Rahmenwerk aus der Sicht praktischer Anwendungen, Schriftenreihe der Landesverteidigungsakademie 2/2010, Wien, 2010

3. HTM3 Pilotanwendung und Evaluierung

Basierend auf dem im vorherigen Kapitel beschriebenen META-Modell erfolgt in diesem Kapitel die konkrete Umsetzung dieses Modells für das Projekt „Zukünftige Technologien im Kontext hybrider Bedrohungen und deren sicherheitspolitischer Auswirkungen auf Staat, Gesellschaft und Sicherheitskräfte - Risiken und Lösungsansätze".
In den folgenden Subkapiteln werden die Ergebnisse und Vorgehensweisen dahingehend beschrieben.

3.1. Operationalisierung der Akteure

Ausgehend von dem in Kapitel 0 entwickelten Modell werden Akteure für die Pilotanwendung unter Berücksichtigung der Rahmenbedingungen (möglichst realistisch, begrenzte Tiefe und möglichst relevant), wie folgt kategorisiert:

- Staatliche Akteure Österreich (vollständig zu erfassen)
- Staatliche Akteure sonstige Staaten (nicht vollständig zu erfassen)
- Nichtstaatliche Akteure (nicht vollständig zu erfassen)

Für die Bearbeitung des gegenständlichen Projektes wurde der Fokus auf die staatlichen Akteure Österreichs gelegt, da diese vollständig aus einer Adhoc Erhebung zu erfassen sind. Die Vorgehensweise der Identifikation und strukturierte Dokumentation der anderen Akteure kann sinngemäß erfolgen.

Grundsätzlich sind staatliche Akteure hier definiert als Akteure, welche die Interessen des Staates umsetzen.
In der nachfolgenden Abbildung 18 sind die nationalen Akteure in einer MindMap schematisch strukturiert dargestellt. Diese Akteure wurden basierend auf den verfügbaren öffentlich zugänglichen Websites identifiziert und stellen potenziell relevante Stakeholder dar.

Abbildung 18 – Staatliche Akteure Österreichs (eingeklappte Darstellung – MindMap)

Bezogen auf die identifizierten österreichischen Akteure, stellen diese jenen Personenkreis aus relevanten österreichischen Organisationen dar, welcher für die operative Weiterbearbeitung dieses Modelles ausgewählt werden muss.

3.2. Handlungsfelder

Die Identifikation der Handlungsfelder wurde entsprechend der nachfolgenden Fragestellung durchgeführt.

Auf welchen Gebieten (Handlungsfelder) können Akteure (staatlich oder nicht staatlich) auf andere Akteure (staatlich oder nicht staatlich) einwirken bzw. Einfluss nehmen?

Folgend dem entwickelten Modell wird grundsätzlich zwischen globalen und nationalen Handlungsfeldern unterschieden. Für die Bearbeitung des gegenständlichen Projektes wurden grundsätzlich die nationalen Handlungsfelder bearbeitet. Die Identifikation der globalen kann jedoch analog zur Identifikation und Dokumentation der nationalen Handlungsfelder erfolgen.

In der nachfolgenden Abbildung sind die identifizierten nationalen Handlungsfelder visuell in Form einer MindMap dargestellt.

Abbildung 19 – Nationale Handlungsfelder (Darstellung – MindMap)

Die Handlungsfelder, welche in 15 Kategorien eingeteilt sind, wurden wie bereits in Kapitel 0 beschrieben im Zuge mehrerer Iterationsschritte aktualisiert und angepasst. Weitere Adaptierungen müssen bei konkreten Umsetzungen als iterativer Anpassungsprozess vorgesehen werden.
Die Handlungsfelder sind für jeden Anlassfall spezifisch zu analysieren und darzustellen. Diesbezüglich sind die Handlungsfelder in der vorhergehenden Abbildung schematisch visualisiert.

Basierend auf unterschiedlich vorliegenden Dokumenten[40, 41] und Wissensständen erfolgte die Adaption und Konzeption für die gegenständliche Bearbeitung im Projekt.

3.3. Use Case Identifikation

Zielsetzung in diesem Schritt ist es unterschiedliche Use Cases zu erhalten, die einer vertiefenden Analyse unterzogen werden. Die Frage, was als Use Case in Betracht gezogen werden kann und was nicht, stellt sich hierbei nicht, da eine Auswahl im Testszenarium idealerweise verschiedene Varianten mit einer möglichst großen Varianz berücksichtigt. Sämtliche von Experten als relevant identifizierten Ereignisse stellen grundsätzlich einen geeigneten Use Case dar. Das Ziel in diesem Schritt ist also nicht die Bewertung von Ereignissen, sondern vielmehr die strukturierte Dokumentation von möglicherweise relevanten Ereignissen.

Die Experten (siehe Kapitel 3.1) erhalten Zugang zu einem webbasierten Erfassungs- und Dokumentationstool und sind in der Lage innerhalb von wenigen Minuten ein Ereignis als Use Case strukturiert anzulegen und dadurch für die weiteren Analysen verfügbar zu machen.
Die Funktionsweise bzw. Inhalte des webbasierten Erfassungs- und Dokumentationstool stellen sich wie in Abbildung 20 visualisiert dar.

[40] Vgl. Anton Dengg, Michael Schurian (Hrsg.). Vernetzte Unsicherheit Hybride Bedrohungen im 21. Jahrhundert. Schriftenreihe der Landesverteidigungsakademie, Band 6/20216, Wien, 2016

[41] Vgl. Joachim Klerx, Cyber Threat Assessment, in EDA Cyber Defence Technology Landscaping, 2022, adaptiert und neu recherchiert für den Kontext hybrider Bedrohungen

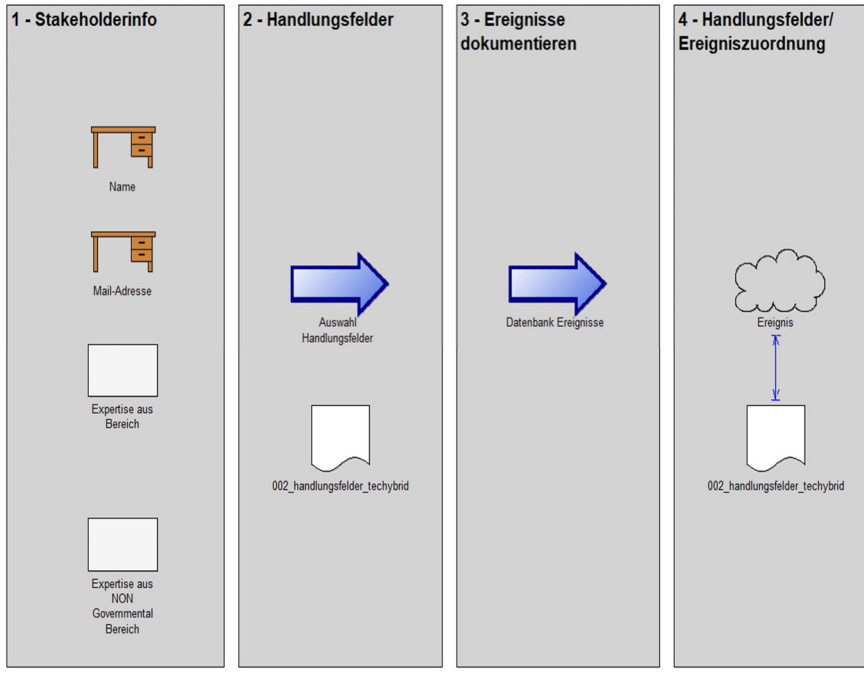


Abbildung 20 – Strukturmodell des webbasierten Erfassungs- und Dokumentationstool[42]

Neben den relevanten Informationen der Stakeholder welche grundsätzlich einmalig anzugeben sind und dem Profil des jeweiligen Experten entsprechen, gilt es auch einmalig die spezifisch relevanten Handlungsfelder durch jeden Experten zu identifizieren.
Die Ereignisse werden strukturiert zu einem fixen Zeitplan oder anlassbezogen im dritten Schritt dokumentiert und nachfolgend im letzten Schritt mit sämtlichen Handlungsfeldern abgestimmt, basierend auf der vorhandenen Expertise.
In der nachfolgenden Abbildung 21 ist die Struktur des Datenblattes für die Erfassung der Ereignisse dargestellt.

[42] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

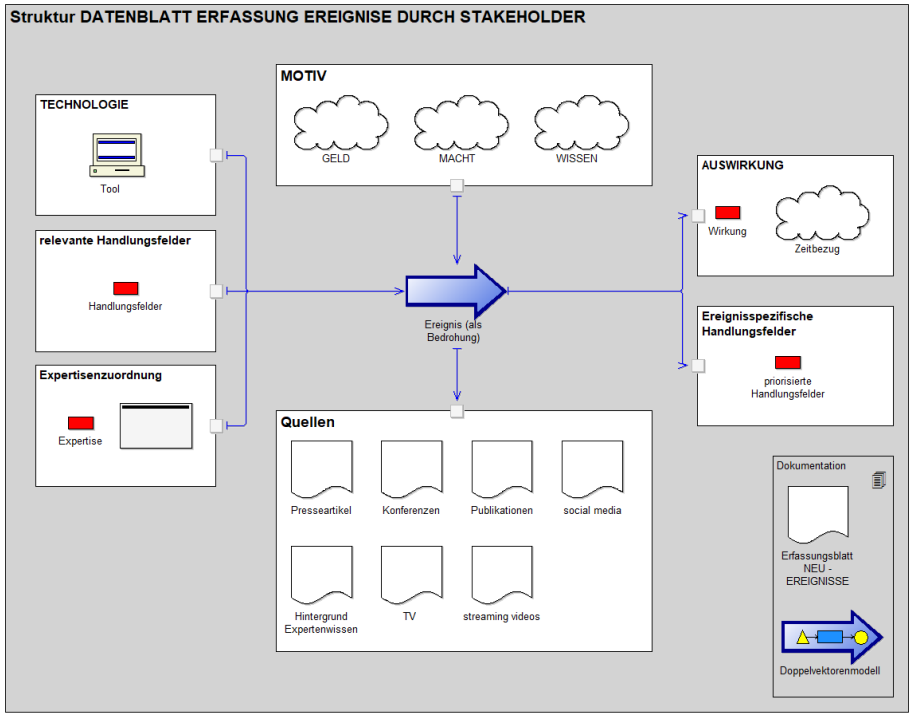


Abbildung 21 – Strukturmodell Datenblatt Erfassung Ereignisse[43]

Ausgehend von einem Ereignis erfolgt die auf Expertenwissen basierte, strukturierte Dokumentation von Metadaten sowie freie Assoziationen für die nachfolgenden Analysen.
Im Rahmen des Projektes wurde zuerst mit einem excelbasierten Erfassungs- bzw. Erhebungsbogen gearbeitet, welcher kontinuierlich adaptiert wurde. Durch die häufige Anwendung im Rahmen der verschiedenen Testungen, wurde als durchschnittliche Bearbeitungszeit eines Ereignisses 10 Minuten identifiziert. Basierend auf diesen Erfassungs- bzw. Erhebungsbogen, wurde ein Datenbankmodell generiert, welches als Webapplikation von Seiten der ZentDok derzeit als Testversion betrieben wird.

[43] Quelle: eigene Darstellung mit WM-Werkzeug PBM Adonis Promote der ZentDok

3.4. Ereignis Datenbank

Basierend auf den Ergebnissen der Use Case Bearbeitung wurde das Modell einer Datenbank generiert um die Ereignisse, welche einen Use Case darstellen, zu dokumentieren.
Relevant hierbei ist es NICHT die Entscheidung zu treffen inwieweit ein Ereignis als Use Case geeignet ist (siehe Kapitel 3.3). Vielmehr dient die Datenbank zur raschen und strukturierten Erfassung der Ereignisse.
In der nachfolgenden Abbildung 22 ist die Struktur des Erfassungs- bzw. Erhebungsbogen als MindMap visuell dargestellt.
Diese Erfassungssystematik ist die Grundlage für die weiteren Analysen.

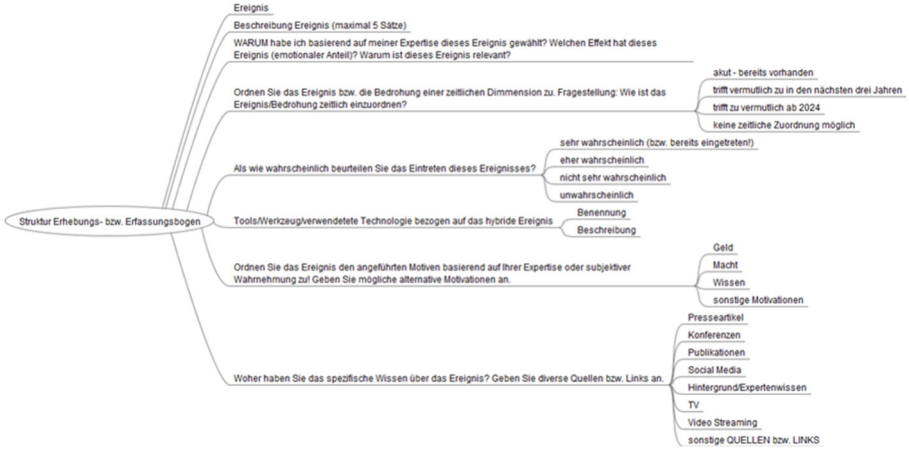


Abbildung 22 – Struktur Erhebungs- bzw. Erfassungsbogen (Darstellung – MindMap)

3.5. Matrizendarstellung

Bei der Matrizendarstellung handelt es sich um eine zweidimensionale Darstellung in Form von Tabellen und Matrizen.
Sämtliche Inhalte, welche durch die Experten zur Verfügung gestellt wurden, werden in verschiedene Matrizen übertragen. Dadurch erfolgt erstmals die objektivierte Darstellung von Ereignissen und Handlungsfeldern.

Die Matrizendarstellungen stellen die Grundlage für die weiteren statistischen- und Netzwerk-Analysen dar. In der nachfolgenden Abbildung ist die Matrix „Auswertung Tools/Werkzeuge“ visualisiert. Bei dieser Matrix handelt es sich um den Proof of Concept für die Identifikation der verwendeten Tools und Werkzeuge im Rahmen der Use Cases während einer der Testphasen.

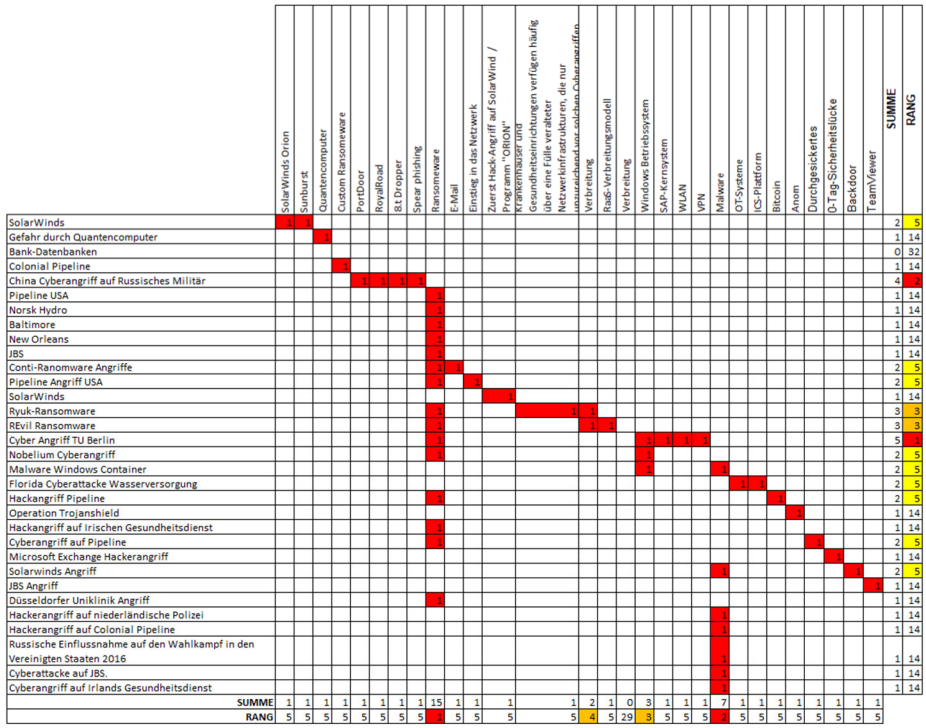


Abbildung 23 – Auswertung Tools/Werkzeuge – Proof of Concept

Neben den Tools und Werkzeugen, welche strukturiert den Ereignissen zugeordnet dargestellt werden, sind sämtliche anderen Inhalte verknüpft mittels der zweidimensionalen Darstellung verfügbar.

3.6. Analyse Matrizen

Die verfügbaren Matrizen werden in weiterer Folge statistisch und mittels 1-mode und 2-mode Netzwerkanalysen mit den Zentralitätsmassen Betweeness, Closeness und Degree analysiert.

In der nachfolgenden Abbildung 24 ist der Proof of Concept des Zusammenhanges der Ereignisse und die Handlungsfelder bezogen auf die unterschiedlichen Bedarfsträger dargestellt. Auf der Y-Achse sind sämtliche Handlungsfelder, auf der X-Achse die aktuell verfügbaren Ereignisse (Use Cases), welche von den unterschiedlichen Bedarfsträgern identifiziert wurden, dargestellt. Die Vernetzung erfolgte durch die Eingaben im Zuge der Tätigkeiten in Modul 3.2. Sowohl die Zusammenhänge als auch die NICHT-Zusammenhänge, werden durch diese Darstellung eindeutig erkennbar.

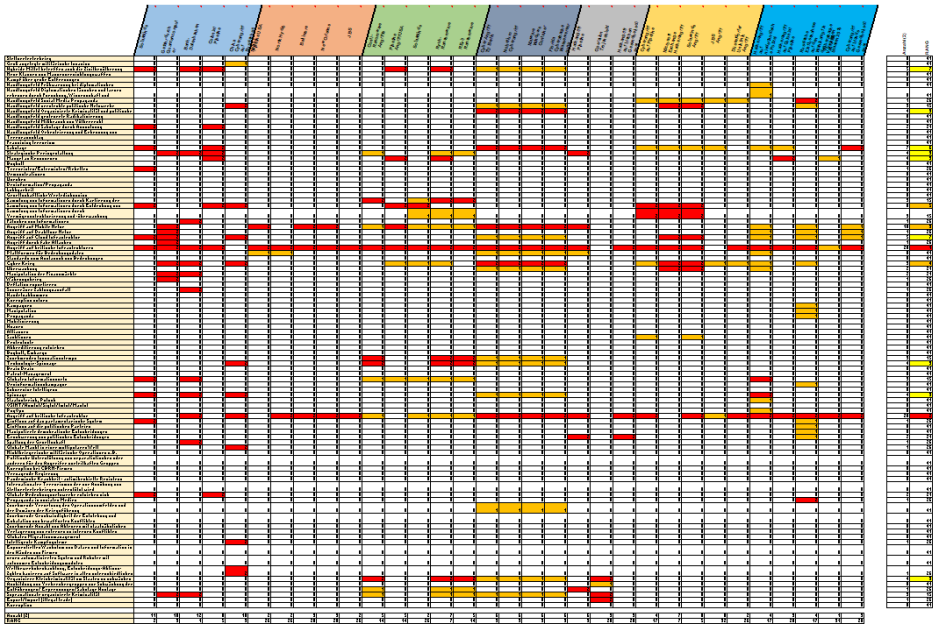


Abbildung 24 – Auswertung Ereignisse und Handlungsfelder sowie Stakeholder – Proof of Concept

Auch hierbei handelt es sich um eine schematische Darstellung, in welcher die Zusammenhänge zweidimensional visualisiert sind.

In der nachfolgenden Abbildung 25 ist die Netzwerkanalyse der identifizierten Tools und Werkzeuge, welche im Rahmen der erfassten Use Cases zum Einsatz kamen, dargestellt. Im Rahmen dieser Analyse wurde das Zentralitätsmaß Degree verwendet. Die Degree Zentralität einer Entität misst die Anzahl der Beziehungen, über die der Knoten verfügt. Im gegenständlichen Fall wird die Größe der Knoten entsprechend dargestellt. Neben der Größe wird auch die Vernetzung (und damit auch die NICHT-Vernetzung) visuell dargestellt.

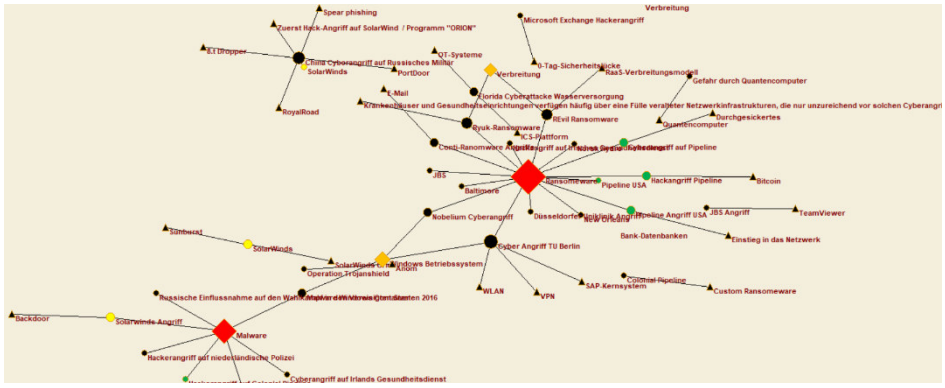


Abbildung 25 – Auswertung Tools/Werkzeuge – Zentralitätsmaß Degree – Proof of Concept[44]

Im Rahmen der Projektbearbeitung wurden unterschiedliche Zentralitätsmaße für die weiterführende Analyse herangezogen. Die vorhergehende Abbildung visualisiert die festgestellten Abhängigkeiten im Rahmen des Proof of Concept schematisch.

[44] Darstellung der vernetzten Abhängigkeit mit dem Open Source Werkzeug PAJEK

Mittels der Matrizendarstellung sind somit die verschiedensten Analyseergebnisse verfügbar (Auszug):

- Zusammenhang von Handlungsfeldern und Ereignissen
- Zusammenhang von Handlungsfeldern und Bedarfsträgerorganisationen
- Zusammenhang zwischen Ereignissen und verwendeten Tools /Werkzeugen

Zusätzlich ermöglicht es diese Darstellung sowie die Anwendung der Analysetools, die Ergebnisse in Zeitreihen darzustellen und weiter zu analysieren.

Durch die Anordnung verschiedenster Matrizenlayer entsteht die Möglichkeit einer mehrdimensionalen Betrachtung, was wiederum die Grundlage für Maschine Learning- und/oder KI-Anwendungen darstellt.

3.7. Expertenpool

Wie bereits im Kapitel 3.1 beschrieben, wurden im Rahmen von mehreren Workshops und Interviews verschiedenste Experten eingeladen, um den jeweiligen Entwicklungsstand des Modelles zu testen und zu diskutieren.
Der Expertenpool, welcher in mehreren Iterationen die Testung durchführte und erste Inhalte bereitstellte, setzte sich aus unterschiedlichen Experten aus nationalen Behörden sowie Forschungseinrichtungen zusammen.

Teilweise wurden für interne Systemtestungen auch die Mitarbeiter des CDFZ der ZentDok herangezogen. Sämtliche Prozessschritte und Feedbackloops wurden dabei separat dokumentiert und die Erkenntnisse unmittelbar in das Modell im Sinne eines adaptiven Prozesses, der iterativ verbessert wird, integriert.
Ausgehend von den Ergebnissen der unterschiedlichen Matrizen, kann sich der Bedarf an weiteren Experten der unterschiedlichen Domains ergeben.

Diese wären in weiterer Folge in den Expertenpool aufzunehmen, damit Ihre Expertise transparent verfügbar ist.

3.8. Delta-Analyse

In diesem Schritt erfolgten die Analyse und Priorisierung von identifizierten Ereignissen und die dazugehörige Technologie mit einem Einfluss auf den Staat Österreich.
Die Delta-Analyse beinhaltet den Content der globalen Handlungsfelder sowie der Expertise aus dem Expertenpool.
Das Ergebnis der Delta-Analyse stellt hier die als kritisch identifizierten Prozesse für ein priorisiertes Ereignis in den relevanten Handlungsfeldern dar.

Die Delta-Analyse stellt die Grundlage für die im Meta-Modell beschriebene Risikoanalyse (Modul 4.5) dar. Die Risikoanalyse sowie das anschließende Modul 4.6 „Operatives Handlungsmodul" wurden im Zuge des Projektes nicht mehr durchgeführt, da aufgrund der vorliegenden Expertise der ZentDok dieser Proof of Concept vorweggenommen wurde und kein weiterer Erkenntnisgewinn aus der Durchführung der Analyse zu erwarten gewesen wäre.

In jedem Fall ist es für das Modell sehr wichtig, dass sowohl positive Erfahrungen als auch negative Erfahrungen erfasst und zu Schulungszwecken dokumentiert werden.[45]

[45] Jan Angstrom, Escalation, Emulation, and the Failure of Hybrid Warfare in Afghanistan STUDIES IN CONFLICT & TERRORISM 1057-610X 2017 10.1080/1057610X.2016.1248665

4. Zusammenfassung HTM3

Wie in der Einleitung bereits erwähnt, gilt es, frühzeitig Analysemodelle zu generieren, um sich zeitgerecht auf neue sicherheitspolitischer Herausforderungen – insbesondere hybrider Bedrohungen – vorzubereiten. Staaten soll damit ihre Handlungsfähigkeit erhalten bzw. gestärkt werden. Das in dieser Publikation vorgestellt HTM3-Meta-Modell stellt eine Möglichkeit dar, Handlungsoptionen frühzeitig einzuleiten, um staatliche Souveränität größtmöglich zu gewährleisten.

Zusammenfassend lässt sich festhalten, das Meta Modell HTM3 mit den einzelnen Modulen verfügbar ist. Das Meta Modell wurde konzipiert, um der aktuellen europäischen Sicherheitsarchitektur Rechnung zu tragen, wie ausführlich im Exkurs beschrieben. Die größte Herausforderung dieser Sicherheitsarchitektur ist, dass ein Rahmen für die effektive Zusammenarbeit der EU-Mitgliedsstaaten geschaffen werden muss, ohne zu viel an souveräner Eigenstaatlichkeit aufzugeben. Das theoretische Konzept der Subsidiarität ist schwierig umzusetzen, wenn bei der Lösung von Konflikten offensichtlich Geschwindigkeit und konsistentes Handeln von vereinten Kräften einen entscheidenden Wettbewerbsvorteil darstellt. Diese Transformationsherausforderung hin zu einer europäischen Sicherheitsarchitektur ist nur politisch zu lösen.

Die Idee zur Konzeption von HTM3 war und ist, die staatliche Handlungsfähigkeit im Bereich hybrider Bedrohungen zu unterstützen und dem Subsidiaritätsprinzip weitestmöglich Rechnung zu tragen.

Das „Proof of Concept" wurde beispielhaft aus der Perspektive eines Nationalstaates (aus pragmatischen Gründen im Rahmen des Projekt Settings: Österreich) mit mehreren Iterationen durchgeführt. Im Kontext dieser Iterationen wurden alle Module kontinuierlich verbessert und so konzipiert,

dass die Anpassung an die nationalstaatlichen Bedürfnisse tunlichst von den Prozessen getrennt wurden, um den Einsatz von HTM3 prinzipiell in jedem Staat zu ermöglichen. Zusätzlich sind die Schnittstellen der Module so definiert, dass der Austausch von Informationen und Wissen möglichst standardisiert ist. Die Ergebnisse evaluierten und diskutierten unterschiedliche Stakeholder und Experten. Damit flossen deren Erfahrungen aus den jeweils anderen Ressorts ein.

Das Modell bietet eine ganze Reihe an Innovationen im Umgang mit hybriden Bedrohungen.

Der „bottom up"-Ansatz bei der Entwicklung des Modells, welches situativ adaptiert werden kann, hat sich bewährt. Es bietet die Voraussetzung für eine Objektivierung der Analyse im Zusammenspiel von Expertenwissen und verschiedensten technischen Errungenschaften (von der Datenaufbereitung bis zur Anwendung von „maschine learning" (ML) und künstlicher Intelligenz. Die Ausrichtung darauf, dass mit jeder neuen identifizierten Bedrohung das Modell verbessert wird, ermöglicht die Darstellung eines umfassenden, domainübergreifenden multidimensionalen Lagebildes. Aus bestehenden Ereignissen für die Zukunft konsistent zu lernen, stellt dabei eine wesentliche Innovation dar. Der hohen Innovationskraft hybrider Bedrohungen wird damit begegnet, was bei bisherigen Modellen und Konzepten nicht möglich war.

Das in dieser Arbeit vorgestellte Modell ist als innovatives Analysetool zu werten. Es ist ausgerichtet auf zukünftige Bedrohungen zur Einschätzung von Risiko- und Bedrohungspotentialen vor allem durch die missbräuchliche Anwendung von neuen Technologien negativ intendierter Akteure. Das ausgearbeitete Modell ist in der Lage, aufgrund seiner Breite, Tiefe und seines Umfanges, ein komplexes multidimensionales Lagebild möglichst objektiv,

rasch und transparent darzustellen, was in dieser Form bisher kaum realisierbar war.

Zur weitestmöglichen Objektivierung der Analysen ist angedacht, die notwendige Datenaufbereitung zunächst durch Expertenwissen zu begleiten, bis entsprechende Algorithmen eine mit „Machine learning" und künstlicher Intelligenz unterstützte Arbeit, größtmögliche Automation und somit Arbeitserleichterung für den Anwender zulässt.

Die Automatisierung ermöglicht Analysten ein kontinuierliches Monitoring von Risiken, was einen „predictive" Ansätze erleichtert. Die Handlungsfähigkeit des Modellanwenders wird massiv verbessert und ein neutraler Abgleich von Chancen und Risken anhand strukturierter Schnittstellen steigert in Folge die Resilienz.

Das vorliegende Modell stand unter dem Motto „Proof of Concept" und die Ergebnisse wurden von unterschiedlichen Stakeholdern iterativ evaluiert.

Hervorzuheben ist, dass dieses Modell als Meta-Modell entwickelt wurde, wenngleich sich das Projektteam aus Simplifikationsgründen mit der Fokussierung auf „neue Technologien" behalf. Dennoch kann - je nach gewünschtem Anwendungsfeld oder Bedarf eines staatlichen Akteurs das Modell adaptiert werden.

Auf Wunsch kann durch die Modellentwickler das Modell bei entsprechenden Bedarfsträgern vorgestellt bzw. näher erläutert werden.

Eine Weiterentwicklung dieses Modells – insbesondere durch die Anwendung von KI – ist notwendig und durch Folgeprojekte sicherzustellen.

5. Internationale Anknüpfungspunkte und Ausblick

Der Ukraine-Krieg[4647] hat verdeutlicht, wie notwendig Analysesysteme auf der Grundlage des HTM3 Meta Modells sind. In den letzten Monaten vor dem Krieg stiegen die in den Medien gemeldeten Ereignisse hybrider Bedrohungen exponentiell, sowohl in Bezug auf die Häufigkeit als auch die Varianz. Ohne ein entsprechendes Analyse-Modell ist weder eine **Lagebild Erstellung für die taktische Reaktion,** noch eine **Trendanalyse** und schon gar keine **Foresight Analyse für die strategische Planung** möglich. Durch die hohe Anzahl von unterschiedlichen Propagandamaßnahmen und die beidseitig systematisch verzerrten Pressemeldungen sind **westliche kritische Infrastrukturen mehr als herausgefordert**. Zudem besitzen unabsichtlich in Umlauf gebrachte Informationen die Macht, unbeabsichtigte Wirkungen zu entfalten. Die große Vielfalt hybrider Taktiken, die kurz vor und nach dem Angriff auf die Ukraine sichtbar wurden, offenbaren die aktuellen Taktiken und Fähigkeiten der involvierten staatlicher Akteure. In Europa wurden wieder einmal vor allem die Schwächen der **Gemeinsamen Außen- und Sicherheitspolitik (GASP)** und der **Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP)** deutlich. Der seit 50 Jahren andauernde politischer Prozess, festzulegen wieviel Autonomie in der Außen- und Sicherheitspolitik tatsächlich an EU-Institutionen abgegeben wird und wieviel Autonomie bei den Nationalstaaten der EU verbleibt, bietet eine weitere **offene Flanke für hybride Aktionen**. Der Prozess an sich ist schon eine Herausforderung für die EU-Staaten, da die Sicherheits- und Verteidigungspolitik eine Kernaufgabe eines jeden Staates ist. Autonomie abzugeben

[46] Bazaluk Oleg; Balinchenko Svitlana, Dynamic Coordination of Internal Displacement: Return and Integration Cases in Ukraine and Georgia, MAY 2020, 10.3390/su12104123

[47] Bodziany Marek; Kocon Pawel, IVAN AT THE GATES! - ARMED CONFLICT IN UKRAINE AND THE MORAL PANIC IN POLAND?, TRAMES-JOURNAL OF THE HUMANITIES AND SOCIAL SCIENCES 1406-0922, 2018, 10.3176/tr.2018.2.03

ist keineswegs selbstverständlich und stößt auf unterschiedlichsten Ebenen auf Widerstände. Um die Aufgaben einer ASP auf EU-Ebene lösen zu können, müssen zeitgleich erst einmal Institutionen gegründet werden, die die Aufgaben lösen könnten, damit eine Übertragung von Autonomie überhaupt in Frage kommt. Die EU-Staaten müssen zu der Überzeugung kommen, dass die Übertragung an Autonomie einen Vorteil bietet, weil die Aufgaben dort besser gelöst werden können und die Prozesse dürfen nicht verhindern, dass nationale Interessen soweit sich in der GASP wiederspiegeln, dass nicht einzelne EU Staaten grob benachteiligt sind. Der Prozess selbst ist gut dokumentiert[48], aber die aktuellen Anknüpfungspunkte zu Adressierung hybrider Bedrohungen sind nicht offensichtlich. Deswegen fasst die nachfolgende Graphik die Akteure zusammen, die eine Rolle in der Abwehr hybrider Bedrohungen haben. Nachdem die administrative Ausdifferenzierung der EU noch nicht beendet ist, sind Änderungen in dieser Struktur auch in Zukunft zu erwarten und die Graphik spiegelt eine Momentaufnahme in 2023 wider. NATO und Interpol wurden aufgenommen, weil viele EU-Staaten NATO Mitglied sind und alle EU Staaten mit Interpol kooperieren.

[48] vgl. https://www.europarl.europa.eu/factsheets/de/sheet/158/eu-au%C3%9Fenpolitik-ziele-mechanismen-und-ergebnisse

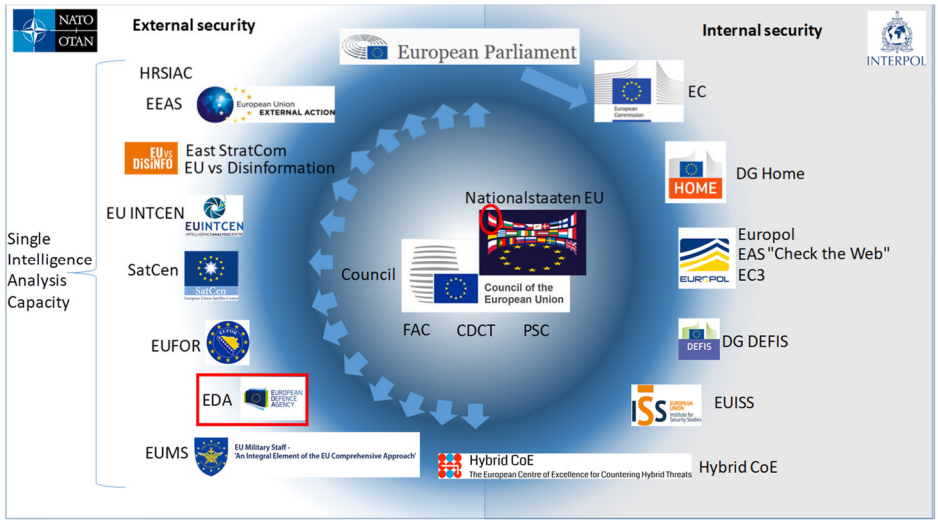


Abbildung 26 – Akteure zur Abwehr hybrider Bedrohungen [49][50]

Die zentrale Stelle für die operative Reaktion auf hybride Bedrohungen in der EU ist die Infrastruktur **„Single Intelligence Analysis Capacity“** mit dem High Representative of the Union for Foreign Affairs and Security Policy (HR) an der Spitze des EEAS und umgebenden administrativen Organisationen.

Besonders hervorheben lassen sich die Organisationen **EU INTCEN**, die u.a. für den operativen Umgang mit hybriden Bedrohungen betraut ist und **Hybrid CoE**[51], welches das EU-Kompetenzcenter für die Abwehr hybrider Bedrohungen ist. Dieses wurde mit einem MoU ins Leben gerufen[52]. “EU-HYBNET (Empowering a Pan-European Network to Counter Hybrid

[49] Ursprüngliche Quelle: Klerx, DANTE 2017, interne Arbeitsunterlage WP11, Update 2023

[50] Die vollständigen Namen der Akteure befinden sich im Abkürzungsverzeichnis.

[51] https://www.hybridcoe.fi/

[52] https://www.bundeskanzleramt.gv.at/dam/jcr:0d93801f-5e10-4d97-8b82-167380cb12ff/25_31_beilage_NB.pdf

Threats) ist ein Projekt der EU Komission mit dem Ziel die Industrie, Wissenschaft und Praktiker in ein Netzwerk zu integrieren. [53]

Hybrid CoE hat folgendes **konzeptuelle Modell**[54] zur Strukturierung einer Landschaft von hybriden Bedrohungen mit einer **Akteur-, Tool-, Domain-, Aktivitäts- und Zielgliederung** vorgeschlagen, welche gewisse Ähnlichkeiten zum Schema der Ereignis Datenbank von HTM3 hat. Die Innovationen liegen hier im Detail der Operationalisierung.

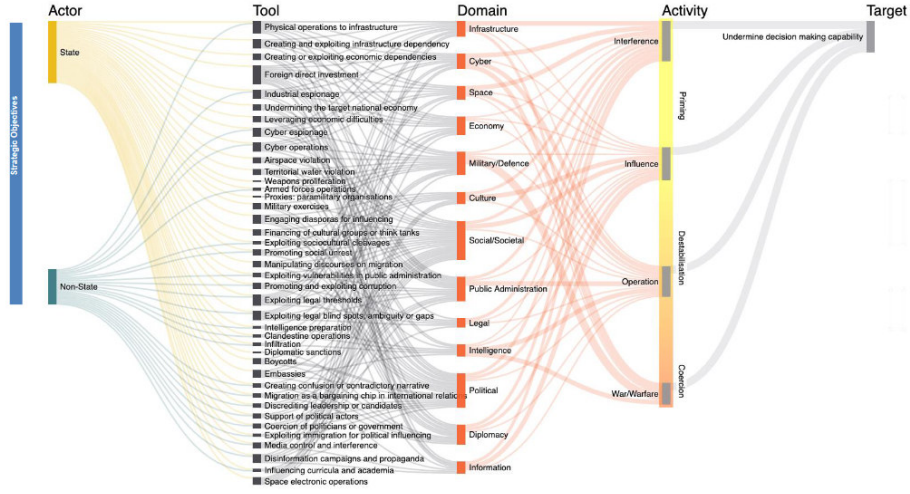


Abbildung 27 – The Landscape of Hybrid Threats[55]

[53] https://euhybnet.eu/about/

[54] Giannopoulos, G., Smith, H., Theocharidou, M, The Landscape of Hybrid Threats: A Conceptual Model, Public Version, JRC123305, EUR 30585 EN, ISBN 978-92-76-29819-9, ISSN 1831-9424, doi:10.2760/44985, 2021, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC123305/conceptual_framework-reference-version-shortened-good_cover_-_publication_office_1.pdf

[55] Giannopoulos, G., Smith, H., Theocharidou, M, The Landscape of Hybrid Threats: A Conceptual Model, Public Version, JRC123305, EUR 30585 EN, ISBN 978-92-76-29819-9, ISSN 1831-9424, doi:10.2760/44985, 2021, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC123305/conceptual_framework-reference-version-shortened-good_cover_-_publication_office_1.pdf

Wie in Kapitel 3.4. beschrieben ist die Erfassung hybrider Aktivitäten in HTM3 strikt Ereignis bezogen, um sicher zu stellen, dass die Informationen über Ereignisse von ideologischen Konzepten unterschieden werden können. Eine „Akteur-, Tool-, Domain-, Aktivitäts- und Zielgliederung", wie von Hybrid CoE vorgeschlagen, könnte aus den Daten der HTM3 Ereignis-Datenbank abgeleitet werden, um eine Landschaft der hybriden Bedrohungstypen zu erstellen. Zur Ableitung staatlichen Handelns ist allerdings auch eine „forensische" Erfassung mit vollständiger Beweiskette notwendig. Dieser Prozess war ein wichtiges Element in der Konzeption der zukünftigen Erfassung hybrider Ereignisse im HTM3 Model.

Ein weiterer Anknüpfungspunkt sind die NATO-Aktivitäten. Schon 2016 hat der HR in einer Mitteilung an Parlament und Rat ein Framework publizieren[56], welches in dem „Gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen" betont, wie wichtig die **Zusammenarbeit mit der NATO** ist. 2018 hat die Kommission in einem Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats eine Spezifizierung der damaligen Aktivitäten an das Parlament und das council geschickt. Mit der Veröffentlichung der neuen EU Security Union Strategy, 2020 hat die Kommission einen neuen Ansatz publiziert, um hybriden Bedrohungen zu begegnen[57]. In diesem werden neben den Akteuren ENISA, Europol und Frontex vor allem auch DEFIS (Directorate-General for Defence Industry and SpaceRolle) genannt, welche gemeinsam mit dem EEAS als point of contact für die Mitgliedsstaaten und externe Stakeholder, wie z.B. das Hybrid Center of Excellence der NATO fungieren.[58] Die NATO

[56] Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen eine Antwort der Europäischen Union, GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT, Brüssel, den 6.4.2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

[57] https://ec.europa.eu/defence-industry-space/eu-defence-industry/hybrid-threats_en

[58] https://ec.europa.eu/defence-industry-space/eu-defence-industry/hybrid-threats_en

accreditierten CoE[59] für Cyber, Terror, Counter Intelligence und Strategic Communication, decken verschiedene Facetten von Hybriden Bedrohungen ab. Das NATO CoE Strategic Communication hat am 8.9.2021 ein „Strategic Communications **Hybrid Threats Toolkit**"[60] veröffentlicht, welches konkret die Erfassung von hybriden Bedrohungen mit folgenden Beispielen anschaulich beschreibt. Der folgende Ausschnitt aus der Liste der Fallstudien zeigt die fallbezogene Erfassung jeweils mit Fall Beschreibung und Themengebiet. Beides wird in HTM3 auch erfasst. Für das Themengebiet verwendet das Hybrid Threats Toolkit allerdings eine allgemeinere Taxonomie als HTM3. Eine Zusammenführung wäre möglich, mit der Anpassung der jeweils verwendeten Taxonomien.

	Case Study	Thematic Area
1	Russian snap exercises in the High North	Coercion through threat or use of force
2	Confucius Institutes	Government Organised Non-Government Organisations (GONGO)
3	2007 cyber attacks on Estonia	Cyber operations
4	US Transit Center at Manas	Economic leverage
5	The spread of Salafism in Egypt	Political actors
6	Disinformation in Sweden	Media
7	Hamas' use of human shields in Gaza	Lawfare
8	The 2010 Senkaku crisis	Economic leverage
9	Humanitarian aid in the Russo-Georgian conflict	Lawfare
10	Chinese public diplomacy in Taiwan	Exploitation of ethnic or cultural identities
11	Detention of Eston Kohver	Espionage and infiltration
12	Finnish airspace violations	Territorial violation
13	South Stream pipeline	Energy dependency

Abbildung 28 – Liste der Fallstudien (Ausschnitt)[61]

[59] https://act.nato.int/application/files/6716/3911/5570/2022-coe-catalogue.pdf.

[60] Monika Gill, Ben Heap, Pia Hansen, Strategic Communications Hybrid Threats Toolkit, ISBN: 978-993456438-3, 2021, https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213

[61] Monika Gill, Ben Heap, Pia Hansen, Strategic Communications Hybrid Threats Toolkit, ISBN: 978-993456438-3, 2021, https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213

Der Ausschnitt aus der Liste der Klassifizierung der Bedrohungen zeigt, wie die Bedrohungen selbst erfasst werden, jeweils mit **Typ der Bedrohung** und **der Prozesslogik**. Diese Erfassung hat den Vorteil, dass über die Zeit hinweg eine Wissensbasis geschaffen wird, die zur taktischen Ausbildung herangezogen werden kann. In HTM3 wird dieses Konzept der Fallstudienbasierten Bearbeitung aufgegriffen und in den Horizon Scanning Prozess integriert, um die Erstellung einer Wissensbasis zu systematisieren.

Type of hybrid threat	Strategic logic
Direct influence of public opinion	- Establishing, funding or supporting academic, educational or cultural institutions. - Misinformation; fake news or disinformation campaigns. - Setting up or supporting media and news channels; media ownerships and advertisement campaigns; pressuring journalists.
Exacerbation of societal divisions	- Funding, supporting or promoting national, religious or political extremist organisations. - Polarisation of political debates to subvert a specific policy programme. - Exploitation of ethnic or cultural identities to undermine social cohesion.
Agitation and civil unrest	- Agitation of a targeted societal, cultural, religious or ethnic group to call for policy change or to initiate protests in targeted nation. - Disruption of political or economic processes through protests or boycotts. - Risk of radicalisation or violent escalation.
Interference in elections	- Foreign interference in elections to influence the voting behaviour of the population.

Abbildung 29 – Liste der Klassifizierung der Bedrohungen (Ausschnitt)[62]

Die Liste der Kommunikationsaktivitäten fasst die Aktivitäten zusammen, die gesetzt wurden, um der Bedrohung zu begegnen, mit den Aktivitäten, das Zielpublikum und die Art der Aktivität. Mit der Erfassung in dieser Ta-

[62] Monika Gill, Ben Heap, Pia Hansen, Strategic Communications Hybrid Threats Toolkit, ISBN: 978-993456438-3, 2021, https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213

belle wurde die Möglichkeit geschaffen, **Auswertungen in Bezug auf Aktivität, Ziel und Maßnahme** zu machen. Damit kann über die Zeit hinweg erfasst werden, welche Akteur bei welchen Maßnahmen mit welcher Aktivität adressiert wurde. Auch dieses ist in HTM3 vorgesehen und wird in der Tabelle der Aktivitäten abgebildet. Eine Zusammenführung wäre allerdings nur möglich, wenn die Taxonomien zu Aktivitäten, Zielen und Maßnahmen harmonisiert wären.

Activity	Target audiences	Measures
"The US sending two carrier strike groups to the Mediterranean Sea will **demonstrate capability** to Russia"[27]	**Adversary** Russian government	Information, Military
"Finland and Sweden conducting a joint exercise to prepare for information influence activities will **reassure home populations"**[28]	**Adversary** Russian government **Domestic** Home populations	Information, Military, Legal (law enforcement)
"The US **sending troops and military equipment** to Saudi Arabia will **reassure** Saudi Arabia and alarm Iran"[29]	**Adversary** Iran **Allies** Saudi Arabia	Information, Military
"Indonesia **deploying fight jets and warships** to patrol Natuna Islands will **deter** Chinese vessels"[30]	**Adversary** China	Information, Military
"Latvia, Estonia and Finland **launching a joint gas market** will **demonstrate** 'energy independence' to Russia"[31]	**Adversary** Russia	Information, Economic
The US **testing interoperability** with NATO allied forces and partners will **reassure Alliance members** and partners[32]	**Adversary** Russia **Allies** NATO alliance members and partner forces	Information, Military

Abbildung 30 – Begleitenden Kommunikationsaktivitäten zu hybriden Aktionen (Ausschnitt)[63]

[63] Monika Gill, Ben Heap, Pia Hansen, Strategic Communications Hybrid Threats Toolkit, ISBN: 978-993456438-3, 2021, https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213

Der Ausschnitt aus der **Liste der Gegenmaßnahmen** zeigt welche Maßnahmen mit welcher Begründung gesetzt wurden. Diese Liste kann in Kombination mit den schon angeführten Listen dahingegend ausgewertet werden, dass deutlich wird, welche Maßnahmen mit welcher Begründung gesetzt wurden und ob diese zu einem Erfolg geführt haben.

Die angeführten Listen wurden primär entwickelt, um **Kommunikationsaktivitäten** zu erfassen. Wie aus der Fallanalyse ersichtlich wurde, weisen hybride Bedrohungen üblicherweise ein ganzes Bündel an möglichen zusätzlichen Aktivitäten auf, die gesetzt werden können. Deswegen ist es ein kritischer Erfolgsfaktor, Aktivitäten hybrider Bedrohungen möglichst frühzeitig und zur Gänze zur identifizieren. Das erfordert eine **Struktur zur Frühwarnung und vorbereitete Fähigkeiten, um diesen Bedrohungen zu entgehen**.

Measure	Rationale
- Industrial espionage; Corporate espionage and illegal technology transfers	- Economic advantage
- Agitation to protest; agitation to sabotage critical infrastructure	- Coercion - Polarisation
- Kidnapping and unlawful detention	- Coercion - Create uncertainty - Plausible deniability
- Espionage; military intelligence gathering; reconnaissance to test resilience	- Reconnaissance to test resilience
- Infiltrating politics, academia and news media by placing intelligence agents or recruiting employees and figures	- Infiltration - Influence decision-making
- Cyber espionage	- Identifying vulnerabilities
- Infiltration of intelligence services	- Intelligence collection of target nation

Abbildung 31 – Liste der Gegenmaßnahmen[64]

[64] Monika Gill, Ben Heap, Pia Hansen, Strategic Communications Hybrid Threats Toolkit, ISBN: 978-993456438-3, 2021, https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213

Das **NATO Toolkit** gibt damit einen einfachen pragmatischen **Rahmen**, um aus **Kommunikationsperspektive hybride Bedrohungen zu analysieren**. Im Unterschied dazu wurde HTM3 entwickelt, um einen taktischen und einen strategischen Vorteil im Kontext hybrider Bedrohungen zu gewinnen. Langfristig soll aus HTM3 ein C2 System für hybride Bedrohungen entstehen. Dazu wird es früher oder später notwendig sein auch domänenübergreifende Eskalation zu integrieren. Dazu bietet es sich an, HTM3 in bestehende C4ISR Systeme zu integrieren.

Die einzelnen in Kapitel 4 getesteten Module von HTM3, können die Konzepte des Strategic Communications Hybrid Threat Toolkits integrieren, sind aber vor allem entwickelt, um als C2 System für hybride Bedrohungen die taktische und strategische Position in der Adressierung hybrider Bedrohungen zu verbessern. Einen wesentlichen Vorteil des HTM3-Modelles stellten dabei die nachvollziehbaren Prozesse dar, die auf die digitale Automatisierung ausgerichtet sind. Hierfür wurde das implementierte Wissensmanagementwerkzeug BPM Adonis Promote für die Modellierung verwendet. Somit liegen die Prozesse transparent vor und sind auf weitere Use Cases übertragbar.

Die zukünftigen Entwicklungsperspektive von HTM3 hängen wesentlich von den Innovationen im Bereich KI ab. Indem die Automatisierung mit KI schon vorbereitet wurde, besteht der nächste Schritt darin, die geeigneten KI-Lösungen zu testen. In den nächsten Jahren ist mit einer Reihe an Innovationen in diesem Bereich zu rechnen, vor allem auch in Bezug auf intelligente Integration[65] Diese Potentiale beeinflussen sowohl die Fähigkeiten,

[65] Burov Oleksandr; Lytvynova Svitlana; Lavrov Evgeniy; Krylova-Grek Yuliya; Orliyk Olena; Petrenko Sergiy; Shevchenko Svitlana; Tkachenko Oleksii M., Cybersecurity in Educational Networks, INTELLIGENT HUMAN SYSTEMS INTEGRATION 2020 2194-5357, 2020,10.1007/978-3-030-39512-4_56

hybriden Bedrohungen zu erkennen, als auch die Fähigkeit auf hybride Bedrohungen effizient reagieren zu können.

Für HTM3 bieten sich in den folgenden in der Graphik dargestellten Modulen, die jeweils zugeordneten schon identifizierten Möglichkeiten, diese mit KI-Einsatz zu verbessern. Konkret wurden schon die in der Graphik angeführten Algorithmen entworfen und getestet, um HTM3 effektiver zu machen. Bei der derzeitigen Entwicklungsgeschwindigkeit ist mit einer ganzen Reihe an zusätzlichen Algorithmen in nächster Zeit zu rechnen.

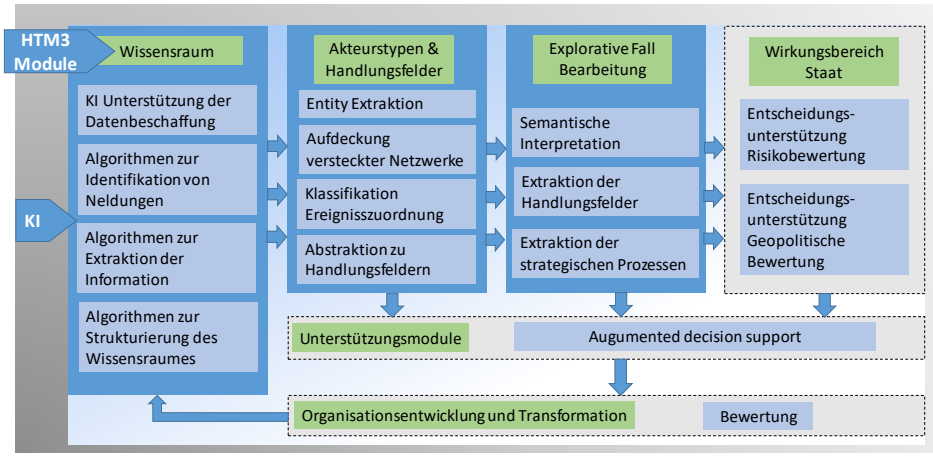


Abbildung 32 – Potentielle KI-Anwendungen innerhalb von HTM3 Modulen

Eine wesentliche Herausforderung von HTM3 ist, dass der Wissensraum unbegrenzt und nicht durchgehend strukturiert ist. Deswegen wurden intelligente Algorithmen zur Datenbeschaffung, Relevanzbewertung und Strukturierung des Wissensraumes getestet, um die Datenbeschaffung zu automatisieren.

Es besonderes Feld der Strukturierung der Information ist die Identifizie-

rung von Handlungsfeldern und Akteursgruppen. Hier wurden spezielle Algorithmen getestet die im EU-Projekt DANTE[66] entwickelt wurden. Eine besondere Herausforderung dabei ist, dass die Einfluss Netzwerke hybrider Bedrohungen üblicherweise mit einem wechselnden Aufwand aktiv verdeckt werden. Deswegen bieten sich Algorithmen an, die eigentlich für die Aufdeckung terroristischer Gruppen entwickelt wurden, wie in DANTE.

Im Modul der explorativen Fallbearbeitung sind Algorithmen zur semantischen Interpretation hilfreich, wie z.B. für die Extraktion von Handlungsfelder und Prozessen. Dabei hat sich herausgestellt, dass die Extraktion von Handlungsfelder deutlich leichter ist als die Extraktion von Prozessen.

Alle folgenden Module könnten vermutlich von einer KI-Unterstützung profitieren. Aber die Algorithmen sind noch in der Entwicklung oder existieren noch gar nicht. Deswegen wurden die Module Wirkungsbereich Staat, Unterstützungsmodule, Organisationsentwicklung und Transformation grau hinterlegt. Es besteht ein entsprechenden Forschungsbedarf zu KI-Modellen in folgendem Kontext:

- Simulation hybrider Bedrohungen
- Entscheidungsunterstützung - Risikobewertung
- Entscheidungsunterstützung – Geopolitische Bewertung
- Augumented decision support (Entscheidungsunterstützung mit „erweiterter Intelligenz“)[67]
- KI unterstützte ergebnisorientierte Bewertung (assessment)

[66] https://www.h2020-dante.eu/

[67] Künstliche Intelligenz und erweiterte Intelligenz haben das gleiche Ziel, aber beziehen sich auf unterschiedliche Verfahren, um ihr Ziel zu erreichen. Beide Techniken nutzen maschinelle Lernfähigkeiten, aber die künstliche Intelligenz verfolgt einen „vollständigen Geräteansatz“, während die erweiterte Intelligenz den menschlichen Aspekt beibehält.

Ergebnisse des Projektes zeigen die Notwendigkeit eines zukünftigen Forschungs- und Entwicklungsbedarfs. Neben der kontinuierlichen Verbesserung der webbasierten Tool-Landschaft, besteht ein Bedarf an Maschine learning (ML) Algorithmen und korrespondierenden ML Semantiken. Langfristig legt das Model HTM3 die Grundlage für ein „Augmented Decision Support System" im Bereich hybrider Bedrohungen. Diese „erweiterte" Version eines Entscheidungs-Unterstützungssystems vereint die Fähigkeiten eines klassischen regelbasierten Systems mit den Methoden des „natural language Processing (NLP)" sowie des ML aus der künstlichen Intelligenz und kombiniert dieses mit aktuellen Echtzeitinformationen. Bei der Entscheidungsunterstützung wurden solche Systeme schon mit Erfolg entwickelt und getestet. Es gibt erste noch relativ unpräzise Ideen, wie diese erweiterten Entscheidungsunterstützungssysteme für das Forschungsmanagement und die Fähigkeitenentwicklung eingesetzt werden können.

HTM3 wurde nicht nur entwickelt, um die aktuelle Lage hybrider Bedrohungen darzustellen, sondern auch um EU-Trends zu erheben und letztendlich auch um Foresight Informationen über zukünftige Trends zu generieren. HTM3 bezieht sich damit auf den „Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen"[68], welcher konkrete Maßnahmen enthält, mit denen sich HTM3 evaluieren lassen würde. Konkret wurden in Maßnahme 4:" Die Mitgliedstaaten … aufgefordert, die Einrichtung eines Kompetenzzentrums für die „Abwehr hybrider Bedrohungen" zu erwägen." Die Entwicklungsziele von HTM3 richten sich zusätzlich an dem Konzept der umfassenden Landesverteidigung aus, bei dem Prävention ein inhärentes Element der wirksamen Verteidigung ist. Deswegen ist die frühzeitige Erkennung ein wichtiges Element des Design Konzeptes.

[68] Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen eine Antwort der Europäischen Union, GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT, Brüssel, den 6.4.2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

Wie auch immer die Weiterentwicklung von HTM3 voranschreitet, bisherige Ergebnisse haben gezeigt, dass die Module geeignet sind sowohl die Organisationsentwicklung als auch die Transformation von Sicherheitsorganisationen zu begleiten.

Über die Rolle und die Verantwortung bei der Abwehr hybrider Bedrohungen gibt es üblicherweise unterschiedliche Perspektiven in einem Staat. Diese unterschiedlichen Perspektiven in den einzelnen Ressorts wurden in den betrachteten Fällen aktueller hybrider Bedrohungen häufig wiederum ausgenutzt. Deswegen ist eine Präzisierung der Rollen bei der Adressierung hybrider Bedrohungen wichtig, um zukünftigen Bedrohungen möglichst konsistent zu begegnen. Innerhalb der EU sind bisher „die Mitgliedstaaten in erster Linie selbst verantwortlich, um auf hybride Bedrohungen zu reagieren. Aber die in den letzten Jahren geschaffene EU weite Infrastruktur kann unterstützen. Dazu ist es jedoch notwendig, dass der Informationsfluss zwischen den Staaten der EU und EU-Organisationen deutlich verbessert und an die Geschwindigkeit eines hybriden Konfliktes angepasst wird. Da in absehbarer Zukunft damit zu rechnen ist, dass die ersten Warnsignale einer hybriden Operation über einen Angriff bei den Mitgliedsstaaten sichtbar werden, sollten innerhalb der Mitgliedsstaaten effiziente Frühwarnsysteme eingerichtet werden, die mit den jeweiligen Gefahren hybrider Bedrohungen in den jeweiligen Staaten korrespondieren. HTM3 kann dazu beitragen das Risikoprofil aufzubauen.

6. Begriffserklärung

In diesem Kapitel werden projektspezifische Arbeitsdefinitionen näher erläutert.

Hybride Kriegsführung

Hybride Kriegsführung ist ein Begriff, der verwendet wird, um Aktivitäten zu beschreiben, die über rein militärische Taktiken hinausgehen und eine innovative Kombination aus militärischer und nicht militärischer Kriegsführung, zur Durchsetzung politischer Macht beschreibt.

Auch wenn viele Konzept der hybriden Kriegsführung[69] schon lange in der Diplomatie und der Außenpolitik, Verwendung finden, so haben die Innovationen im Cyber Bereich doch dazu beigetragen, dass im 21. Jahrhundert eine vollkommen neue Qualität der hybriden Kriegsführung[70] entstanden ist, in der eine Vielzahl unterschiedlicher Taktiken kombiniert werden, die es erlauben simultan und adaptiv auf das Geschehen reagieren. Das Hauptziel dieser Kriegsführung ist es, den Gegner durch eine Kombination von Maßnahmen zu destabilisieren und zu schwächen, die sowohl legal als auch illegal sein können und deren Urheber oft nicht direkt ersichtlich ist. Diese Art der Kriegsführung wird in einer "grauen Zone" geführt, wo es schwierig ist, den Anfang und das Ende des Konflikts klar zu definieren. Ein Schlüsselelement der hybriden Kriegsführung ist die Verwendung von unterschiedlichen Formen der politischen Macht, um Interessen durchzusetzen. Der Begriff "hybride Kriegsführung" wird immer noch kontrovers diskutiert. Einige Experten argumentieren, dass alle Kriege im Wesentlichen hybrid sind, andere hingegen sehen in der Cyber Kompetente der hybriden Kriegsführung eine neue Qualität. Trotz dieser Kontroversen hat der Begriff in den Diskussionen

[69] Mumford Andrew, Understanding hybrid warfare, CAMBRIDGE REVIEW OF INTERNATIONAL AFFAIRS, 0955-7571, OCT 27, 2020, 10.1080/09557571.2020.1837737

[70] Charap Samuel The Ghost of Hybrid War, SURVIVAL, 0039-6338, NOV 2, 2015, 10.1080/00396338.2015.1116147

über moderne Konflikte und Kriege seine aktuelle Bedeutung gefunden.

Politische Macht

Politische Macht im Kontext hybrider Kriegsführung bezieht sich auf die Fähigkeit eines Akteurs (z.B. einer Nation, einer nichtstaatlichen Gruppe, etc.), durch eine Kombination von militärischen, politischen, wirtschaftlichen und informativen Mitteln, seine Interessen durchzusetzen und Einfluss auf andere Akteure auszuüben. Die politische Macht spielt eine entscheidende Rolle in der hybriden Kriegsführung, da sie dazu verwendet wird, sowohl innerhalb als auch außerhalb der militärischen Kriegsführung zu operieren. Sie kann dazu genutzt werden, die öffentliche Meinung zu manipulieren, wirtschaftliche Sanktionen zu verhängen, Diplomatie zu nutzen, um Verbündete zu gewinnen oder Gegner zu isolieren, und vieles mehr. Die Akteure der hybriden Kriegsführung nutzen politische Macht, um ihre strategischen Ziele zu erreichen, oft ohne einen offenen Krieg zu beginnen. Daher äußern sich die Elemente der politische Macht im Kontext der hybriden Kriegsführung in subtiler und komplexer Art und Weise.

Cyber

Cyber bezieht sich auf den Bereich der Computer- und Informationstechnologie sowie aller damit verbundenen Aspekte der digitalen Kommunikation und des Internets. Er umfasst traditionell die Bereiche Cybersicherheit, Cyberkriminalität, Cyberangriffe, Cyberwarfare und den Schutz von digitalen Systemen vor Bedrohungen. Diese Bereiche sind jedoch nicht ausreichend, um die aktuelle Wirkung von Cyber im Kontext der hybriden Kriegsführung zu erfassen. In diesem Kontext lässt sich Cyber besser beschreiben als jede Form der Computer- und Informationstechnologie, die es erlaubt Macht auszuüben oder durch Einsatz von Geldmitteln politische Macht zu erlangen. Neben den genannten Bereichen schließt das auch die kognitive Kriegsführung und alle anderen Arten der politischen Machtdurchsetzung mit ein, die mit Cybermitteln deutlich effizienter und wirkungsvoller geworden sind. Die Methoden der künstlichen Intelligenz, z.B. ermöglichen vollkommen

neue Formen der kognitiven Kriegsführung. Im Bereich der hybriden Bedrohungen können Cyberangriffen auf die KI zur Entscheidungsunterstützung einer militärischen Operation dazu führen, dass sich die eigenen Waffen gegen sich selbst richten. Genauso können gezielte Angriffe auf die KI Infrastruktur eines Landes zur Schwächung der kritischen Infrastruktur beitragen. Cyberangriffe können dazu verwendet werden, Verwirrung zu stiften, Kommunikationssysteme niederschwellig zu stören so dass ein Propagandaeffekt erreicht wird, der unterschwellig die demokratische Ordnung zerstört.
Die Herausforderung von Cyber Attacken im Kontext hybriden Bedrohungen besteht darin, dass sie verschiedene Bereiche und Disziplinen miteinander verbinden. Es erfordert eine enge Zusammenarbeit zwischen den Bereichen Cybersicherheit, Militär, Geheimdiensten, Politik, Wirtschaft und der Gesellschaft insgesamt, um angemessene Maßnahmen zu ergreifen und sich gegen solche Bedrohungen zu verteidigen.

Künstliche Intelligenz

Die Abkürzung KI steht für Künstliche Intelligenz und beschreibt Algorithmen, Maschinen oder Computersysteme, die menschenähnliche Intelligenz zeigen, insbesondere die Fähigkeit, zu identifizieren, Klassifizieren, analysieren, zu lernen, zu verstehen, Probleme zu lösen, Entscheidungen zu treffen und komplexe Aufgaben auszuführen. Deswegen wäre der bessere Name maschinelle Intelligenz. Sie kann im Kontext hybrider Bedrohungen sowohl als Werkzeug zur Abwehr als auch zur Durchführung hybrider Bedrohungen dienen.

Mit Hilfe von KI können z.B. einzelne Menschen gezielt angegriffen werden[71], gefälschte Nachrichten generiert und verbreitet werden, um politische

[71] Haas Michael Carl; Fischer Sophie-Charlotte, The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order, CONTEMPORARY SECURITY POLICY, 1352-3260, , 2017, 10.1080/13523260.2017.1336407

Prozesse zu stören oder zu manipulieren, Verwirrung zu stiften und Misstrauen zu säen. KI kann ebenso zur Durchführung von Cyberattacken eingesetzt werden, z.B. durch automatisiertes Hacking, wie zu vielen anderen Aktivitäten im Kontext hybrider Bedrohungen.

KI kann aber auch zur Bekämpfung von hybriden Aktionen eingesetzt werden, wie, z.B. zur Identifizierung von Falschinformationen oder zur Identifikation manipulierter Medien eingesetzt wird. In der Cyberabwehr kann KI zur Erkennung und Bekämpfung von Cyberangriffen eingesetzt werden, indem sie versteckte Netze der Angreifer aufdecken und Anomalien und Muster im Angriff erkennt und bekämpft. Sie kann auch dazu verwendet werden, Schwachstellen in Systemen zu identifizieren und zu beheben, um zukünftige Angriffe zu verhindern. KI kann in vielen weiteren relevanten Bereichen eingesetzt werden, von Spracherkennung und Bildanalyse bis hin zu autonomen Weak-Signal Erkennung und komplexer Datenanalyse.[72] Deswegen ist die KI eine wichtige unterstützende Disziplin in der Bekämpfung hybrider Bedrohungen und hat das Potenzial bei der Automatisierung der Bekämpfung hybrider Methoden wesentliche Aufgaben zu übernehmen.

[72] Medar Sergiu, Intelligence in Hybrid Warfare, COUNTERING HYBRID THREATS: LESSONS LEARNED FROM UKRAINE, 1879-8268, , 2016, 10.3233/978-1-61499-651-4-50

7. Abkürzungsverzeichnis

AIT	Austrian Institute of Technology
BPM	Business Process Model(ing)
BMLV	Bundesministerium für Landesverteidigung
CATALYST	ColAborative Trend AnaLYtics SysTem
CDCT	Council of Europe Committee on Counter-Terrorism
CDFZ	Cyber Defense Forschungs Zentrum
DG DEFIS	Directorate-General Defence Industry and Space
EAS	Europol Analysis System
East StratCom	East StratCom Task Force
EC	European Commission
EC3	Europäisches Zentrum zur Bekämpfung der Cyber-kriminalität
EDA	European Defense Agency
EEAS	European External Action Service
EU INTCEN	European Union Intelligence Analysis Centre
EUFOR	European Union Force
EUISS	European Union Institute for Security Studies
EUMS	European Union Military Staff

Europol	European Union´s law enforcement agency
FAC	Foreign Affairs Council
HB	Hybride Bedrohungen
HRSIAC	High Representative of the Union for Foreign Affairs and Security Policy
Hybrid CoE	The European Centre of Excellence for Countering Hybrid Threats
HTM3	Hybrid Threat Meta Monitoring Modell
KI	Künstliche Intelligenz
KIRAS	Ist ein Österreichisches Förderprogramm für Sicherheitsforschung
IFK	Institut für Friedenssicherung und Konfliktmanagement
IKKM	Internationales Krisen- und Konfliktmanagement
LVAk	Landesverteidigungsakademie
MilStrat	Abteilung Militärstrategie
ML	Maschine Learning
NATO CoE	NATO CoE Strategic Communication
OSint/OSINT	Open Source Intelligence
Osinfo	Open Source Information
PSC	Politisch sicherheitspol. Komitee
SatCen	European Union Satellite Centre
SIAC	Single Intelligence Analysis Capacity

WPS	Wissens Performance System
ZentDok	Abteilung Zentraldokumentation der Landesverteidigungsakademie
4GW	Fourth-Generation Warfare
ÖBH	Österreichisches Bundesheer

8. Literaturverzeichnis

Alexander Armbruster, Kausalität. Was Künstlicher Intelligenz noch fehlt. Und warum sie dennoch längst nicht nur kommerziellen Erfolg von Misserfolg trennt, sondern auch politisch zu einer zentralen Macht-Variablen geworden ist. Frankfurter Allgemeine Zeitung, Montag, 10. Jänner 2022, Nr. 7

Anton Dengg, Michael Schurian (Hrsg.), Vernetzte Unsicherheit - Hybride Bedrohungen im 21. Jahrhundert, Schriftenreihe der Landesverteidigungsakademie, Band 15/2016, Wien, Juli 2015

Anton Dengg, Michael Schurian (Hrsg.), Vernetzte Unsicherheit - Hybride Bedrohungen im 21. Jahrhundert, 2. überarbeitete und erweiterte Auflage, Schriftenreihe der Landesverteidigungsakademie, Band 6/2016, Wien, Februar 2016

Anton Dengg, Michael Schurian (Eds.), Networked Insecurity - Hybrid Threats in the 21st Century, Schriftenreihe der Landesverteidigungsakademie, Band 17/2016, Wien, Februar 2016

Anton Dengg (Ed.), Tomorrow's Technology. A Double-Edged Sword, Schriftenreihe der Landesverteidigungsakademie, Band 3/2018, Vienna, March 2018

Bazaluk Oleg; Balinchenko Svitlana, Dynamic Coordination of Internal Displacement: Return and Integration Cases in Ukraine and Georgia, MAY 2020, 10.3390/su12104123

Bodziany Marek; Kocon Pawel, IVAN AT THE GATES! - ARMED CONFLICT IN UKRAINE AND THE MORAL PANIC IN POLAND?, TRAMES-JOURNAL OF THE HUMANITIES AND SOCIAL SCIENCES, 1406-0922, 2018, 10.3176/tr.2018.2.03

Burov Oleksandr; Lytvynova Svitlana; Lavrov Evgeniy; Krylova-Grek Yuliya; Orliyk Olena; Petrenko Sergiy; Shevchenko Svitlana; Tkachenko

Oleksii M., Cybersecurity in Educational Networks, INTELLIGENT HUMAN SYSTEMS INTEGRATION 2020, 2194-5357, 2020, 10.1007/978-3-030-39512-4_56

Charap Samuel, The Ghost of Hybrid War, SURVIVAL, 0039-6338, 2015, 10.1080/00396338.2015.1116147

Christine Wahlmüller-Schiller, Künstliche Intelligenz - wohin geht die Reise. In: „Elektrotechnik & Informationstechnik", published: 25 October 2017, S. 364-369

Christoph Bilban, Hanna Grininger (Hrsg.), Mythos "Gerasimov-Doktrin" Ansichten des russischen Militärs oder Grundlage hybrider Kriegsführung?, Schriftenreihe der Landesverteidigungsakademie, Band 2/2019

Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen eine Antwort der Europäischen Union, GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT, Brüssel, den 6.4.2016, JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

Georgios Giannopoulos, The Landscape of Hybrid Threats: A Conceptual Model, Public Version, Luxembourg: Publications Office of the European Union, 2021, European Union and Hybrid CoE, 20212021, ISBN 978-92-76-29819-9, ISSN 1831-9424, doi:10.2760/44985, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC123305/conceptual_framework-reference-version-shortened-good_cover_-_publication_office_1.pdf

Haas Michael Carl; Fischer Sophie-Charlotte, The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order, CONTEMPORARY SECURITY POLICY, 1352-3260, , 2017, 10.1080/13523260.2017.1336407

https://www.europarl.europa.eu/factsheets/de/sheet/158/eu-au%C3%9Fenpolitik-ziele-mechanismen-und-ergebnisse

https://www.hybridcoe.fi/

https://www.bundeskanzleramt.gv.at/dam/jcr:0d93801f-5e10-4d97-8b82-167380cb12ff/25_31_beilage_NB.pdf

https://euhybnet.eu/about/

https://www.h2020-dante.eu/

https://ec.europa.eu/defence-industry-space/eu-defence-industry/hybrid-threats_en

https://act.nato.int/application/files/6716/3911/5570/2022-coe-catalogue.pdf.

https://vpk-news.ru/articles/14632

Jan Angstrom, Escalation, Emulation, and the Failure of Hybrid Warfare in Afghanistan STUDIES IN CONFLICT & TERRORISM 1057-610X 2017 10.1080/1057610X.2016.1248665

Johannes Göllner, Klaus Mak, Robert Woitsch, Grundlagen zum Wissensmanagement im ÖBH. Teil 1: Ein WM-Rahmenwerk aus der Sicht praktischer Anwendungen, Schriftenreihe der Landesverteidigungsakademie 2/2010, Wien, 2010

Klaus Mak, Joachim Klerx, Hans Christian Pilles, Johannes Göllner, Wissensentwicklung mit „Crows OSInfo", Eine Innovation des Cyber Documentation & Research Center (CDRC) der Zentraldokumentation (ZentDok), Landesverteidigungsakademie (LVAk), Schriftenreihe der Landesverteidigungsakademie, 2015

Klaus Mak, Hans Christian Pilles, Markus Bertl, Joachim Klerx, Wissensentwicklung mit IBM Watson in der Zentraldokumentation (ZentDok) der Landesverteidigungsakademie, Entwicklungen und Anwendungen in der Open-Source Informationsbereitstellung des ÖBH, Schriftenreihe der Landesverteidigungsakademie, 2018

Klerx Joachim, Cyber Threat Assessment, in EDA Cyber Defence Technology Landscaping, 2022, adaptiert und neu recherchiert für den Kontext hybrider Bedrohungen

Medar Sergiu, Intelligence in Hybrid Warfare, COUNTERING HYBRID THREATS: LESSONS LEARNED FROM UKRAINE, 1879-8268, 2016, 10.3233/978-1-61499-651-4-50

Monika Gill, Ben Heap Pia Hansen, Strategic Communications Hybrid Threats Toolkit, ISBN: 978-993456438-3, 2021, https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213

Mumford Andrew, Understanding hybrid warfare, CAMBRIDGE REVIEW OF INTERNATIONAL AFFAIRS, 0955-7571, OCT 27, 2020, 10.1080/09557571.2020.1837737

Qiao Liang, Wang Xiangsui, Unrestricted Warfare, PLA Literature and Arts, Publishing House, February 1999

Robert Woitsch, Klaus Mak, Johannes Göllner, Grundlagen zum Wissensmanagement im ÖBH. Teil 2: Wissensbilanz als Steuerungsinstrument im ÖBH: Ein Evaluierungs-Rahmenwerk aus der Sicht praktischer Anwendungen, Schriftenreihe der Landesverteidigungsakademie 10/2010, Wien, 2010

Sean Kimmons, Army strategizing for holistic change, not just new tech, 2017

Rick Meessen, et. all., A HORIZON SCAN OF TRENDS AND DEVELOPMENTS IN HYBRID CONFLICTS SET TO SHAPE 2020 AND BEYOND, 2021, https://euhybnet.eu/wp-content/uploads/2021/06/TNO-HCSS-Horizon-scan-Hybrid-Trends-and-Developments-2002-.pdf

Thomas Pankratz, „Überlegungen zum Begriff „Strategische Bedrohungen", in: Anton Dengg, Michael Schurian (Hrsg.), Vernetzte Unsicherheit - Hybride Bedrohungen im 21. Jahrhundert, 2. überarbeitete und erweiterte Auflage, Schriftenreihe der Landesverteidigungsakademie, Band 6/2016, Wien, Februar 2016

The Joint Air Power Competence Centre, Joint Air & Space Power Conference. Shaping NATO for Multi-Domain Operations or the Future, 2019, Germany, https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf

Tim Sweijs, Samuel Zilincik, Frank Bekkers, Rick Meessen, Framework for Cross-Domain Strategies Against Hybrid Threats, 2021, https://euhybnet.eu/wp-content/uploads/2021/06/Framework-for-Cross-Domain-Strategies-against-Hybrid-Threats.pdf

Volodymyr Zahorskyi, Andriy Lipentsev, Svitlana Andreyeva, Peculiarities of Public Administration Development in Ukraine in the Conditions of Democratic Transition: Status and Instruments VISION 2020: SUSTAINABLE ECONOMIC DEVELOPMENT AND APPLICATION OF INNOVATION MANAGEMENT, 2018

William S. Lind, Gregory A. Thiele, 4th Generation Warfare, 2016, https://archive.org/details/4th-generation-warfare-handbook

9. Abbildungsverzeichnis

10. Autoren und Lektorat

Autoren:
Dr. Anton DENGG; IFK/ZentDok
Oberst des höheren militärfachlichen Dienstes
Leiter des Institutes für Friedenssicherung und Konfliktmanagement (mit der Führung betraut)
anton.dengg@bmlv.gv.at

Dr. Joachim KLERX, AIT
Austrian Institute of Technology
joachim.klerx@ait.ac.at

Ing. Mag. Klaus MAK; ZentDok/LVAk
Oberst des höheren militärfachlichen Dienstes
Leiter der Zentraldokumentation (ZentDok) an der Landesverteidigungsakademie
EU-zertifizierter Informationsexperte (www.certidoc.net)
klaus.mak@bmlv.gv.at

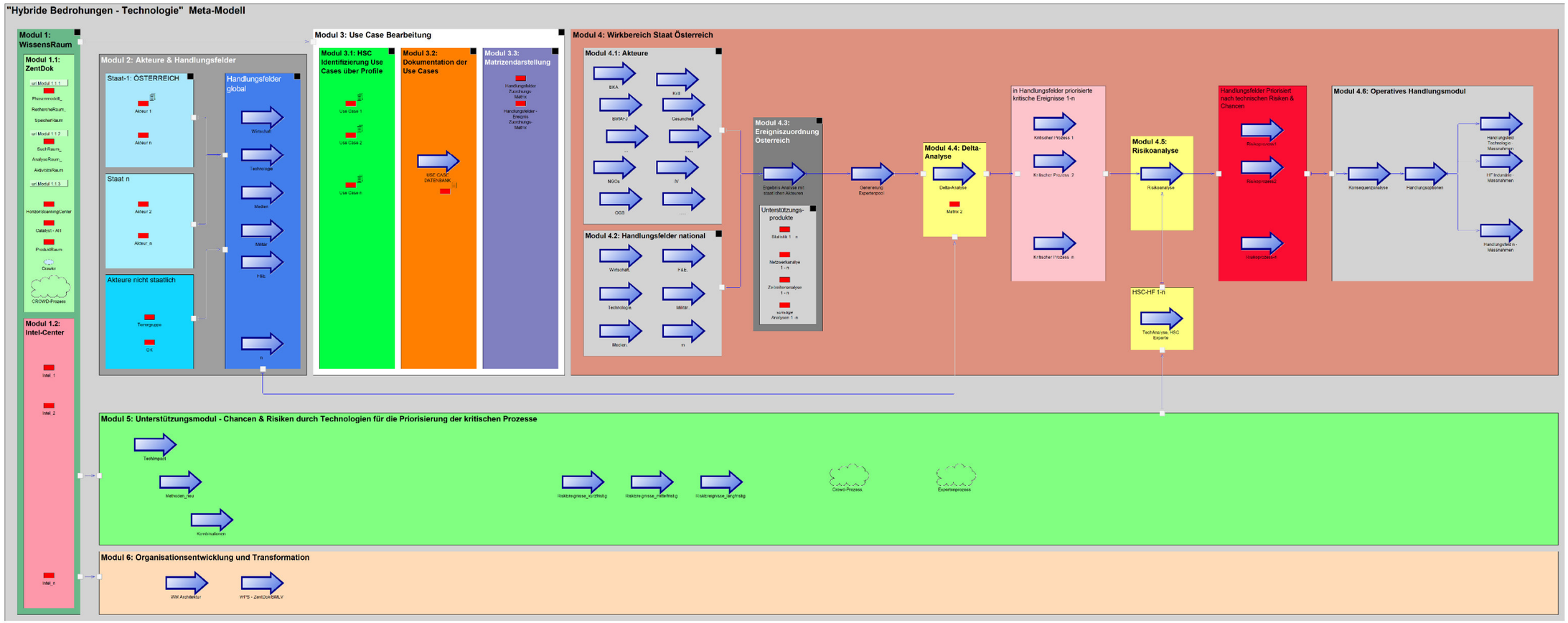
Mag. (FH) Andreas PEER, MBA; ZentDok/LVAk
Oberstleutnant
Offizier für Wissensmanagement an der Zentraldokumentation der Landesverteidigungsakademie
andreas.peer@bmlv.gv.at

Lektorat:
Mag. Rudolf BOGENSPERGER, Bakk.; ZentDok/LVAk
Referent Allgemeine Dokumentation an der Zentraldokumentation der Landesverteidigungsakademie
rudolf.bogensperger@bmlv.gv.at

Karl STOLZLEDERER; ZentDok/LVAk
Referent Wissensmanagement an der Zentraldokumentation der Landesverteidigungsakademie
karl.stolzlederer@bmlv.gv.at

11. Anhang

Hybride Bedrohungen – Technologie Meta-Modell



Band 6 / 2023

Hybride Bedrohungen beschäftigen weltweit Sicherheitspolitiker. Aufgrund unzähliger neuer, zum Teil technologischer Machtmittel und deren Amalgamierung hat sich ein komplexes Bedrohungsbild gebildet. Dies findet mitunter in kreativer und überraschender Art und Weise statt. Daher sind Experten bemüht, entsprechende Analyseverfahren zu entwickeln.

Ein Projekt des Instituts für Friedenssicherung und Konfliktmanagement (IFK) der Landesverteidigungsakademie (LVAk) in Kooperation mit der Zentraldokumentation (ZentDok) der LVAk sowie mit einem Vertreter des Austrian Institute of Technology (AIT) realisierte ein derartiges Analyse-Modell.

Erstmalig wird mit dem in dieser Publikation vorgestellten Meta-Modell ein Horizon Scanning und ein iteratives Analysesystem ermöglicht.

ISBN: 978-3-903359-72-7