Connecting the Dots – Enhancing the Information Processing Chain for the Detection of Hybrid Threats for Host Nation Support and Territorial Operations

Dr. Michael Gerz, Arne Schwarze, Hans Peter Stuch
Fraunhofer FKIE
GERMANY

{michael.gerz|arne.schwarze|hans-peter.stuch}@fkie.fraunhofer.de

ABSTRACT

Hybrid activities are those imposed by orchestrated attacks in multiple domains of operation, including cyber and information warfare. A key challenge in detecting hybrid threats is to recognize individual incidents as the effect of (orchestrated) adversary measures and to correlate allegedly unrelated events. The task to connect the dots is made more difficult by the fact that operations in the physical and the cyber and information domain may take place at different times, at different locations, with different speed, as either short-term or long-term activities, and possibly at low level of intensity. In order to identify information that is relevant to specific mission planning and execution, risk assessment for hybrid threats must always be made in the context of a specific mission with its mission objectives, its area of operation, and its mission timespan.

In this paper, we describe two scenarios in which adversaries may run attacks in both the physical as well as the cyber and information world to disturb an operation. Next, we describe a high-level architecture of a demonstrator that shows how different types of sensors and information sources can be linked together. To counter hybrid threats and to exploit the full potentials of support to analysts and decision makers, it is necessary to achieve situational awareness on different level of details – ranging from raw data to highly aggregated risk assessments –, to share information across the different domains, and to fuse them on an aggregated level.

1.0 INTRODUCTION

Multi-Domain Operations (MDOs) are not a new phenomenon. In warfare, operations have taken place in multiple domains for a long time. Starting with land, naval, and air ops, the space and cyber domains complemented the adversaries' portfolio. To counter these, intensive cooperation of different branches was required. Similarly, the term *Hybrid Threats* is not an invention of the 2020's. Starting out as *hybrid warfare*, it mingled in with concepts like asymmetric warfare, irregular forces, and information operations.

In the early days, the focus was on classic military conflicts. The battlefield was the traditional ground, where tanks, airplanes, and ships in conjunction with the personnel were the main actors. Communication contributed as a key factor to the decision of being the winner or loser. The beginning of digitization offered new benefits and options – but also new vulnerabilities to warfare. The use of what is named *Cyber and Information Domain* (*CID*) today was a big push in terms of military capabilities. With the appearance of social media, the information domain has changed drastically as it makes it far easier for adversaries to influence the public opinion and the opinion of key individuals. In addition, the importance of cyber threats has increased with the growing numbers of inter-connected devices in the Internet of Things. Today's critical infrastructures (for energy, transport, health, etc.) are far more susceptible to IT threats than they used to be and they are popular targets in modern warfare. This opens the door for attacks by opposing forces. Their toolbox is no longer limited to classic military assets. Of course, the emerging technologies resulted in counter and counter-counter measures and an everlasting competition.

The increasing use of and the dependency on information exchange in the military as well as the civilian world spawned new attack vectors and with these also new needs for defence against them. In today's conflicts, threats affect the political, military, economic, social, information, and infrastructural domains. The different threats may be caused by regular and irregular forces. These can be adverse nations as well as groups taking their motivations from non-governmental considerations.

A key challenge is to recognize individual incidents on the tactical level as the effect of (orchestrated) adversary measures and to correlate allegedly unrelated events. 'Is a communication blackout just the result of a technical fault or do you suffer from a targeted cyber attack against your communication infrastructure?' – In risk assessment for mission planning or in mission execution, the answer to this question may result in different decisions for own measures like use of communication channels, force protection, route planning, or counter cyber operations. The task to connect the dots is made more difficult by the fact that operations in the physical and the cyber and information domain may take place at different times, with different speed, as either short-term or long-term activities, and possibly low intensity.

Due to the heterogeneity of threats, the timelines underlying their application are specific and thus different. The use of physical forces happens at a certain time – not earlier, not later. Activities like disinformation campaigns require much longer periods. Moreover, hostile activities are not necessarily geographically related. For instance, the direction of an unmanned aerial vehicle (UAV) can be determined precisely in time, location, and accuracy within the sensor's range and in real time. In contrast to this, for actions in the cyber and information domain, the time and location of impact on the physical world are shifted. The huge variety regarding time, location, and relevance of information poses a big challenge. To force the difficulties on the victim's side, activities can additionally be tailored in grey areas of the law and other regulations. Examples are attacks below the conflict threshold, as well as attacks that are targeting aspects, which are not clearly within the scope of certain branches. To camouflage operations, each individual threat may be conducted on a low level of intensity. But in combination, they can pose a serious risk for the attacked target.

The following descriptions and statements are based on findings gained in a project called *Detection of Hybrid Threats for Urban Operations*. The project uses a wide variety of sensors available at Fraunhofer FKIE and combines these in a demonstrator. In this project, two scenarios describe the operational environment in which adversaries may run attacks in both the physical as well as the cyber and information world to disturb an operation. The first scenario deals with force deployment and focuses on a host nation support mission for allied force transition. The second scenario is about a public military ceremony, a territorial operation in collaboration with national civil authorities. The detection and assessment of hybrid threats for these scenarios was covered by a technical solution. In the following sections, a high-level architecture of the demonstrator shows how different types of sensors and information sources can be linked together.

When coming to data analytics and aggregation, different applications of Artificial Intelligence (AI) and Big Data analyses can be integrated. Presently, these analyses are mostly conducted on the edge, i.e., close to the information sources and within the individual domains. To counter hybrid threats and to exploit the full potentials, it is necessary to achieve situational awareness on different level of details – ranging from raw data to highly aggregated risk assessments –, to share information across the different domains, and to fuse them on an aggregated level. This also requires multi-domain interoperability solutions that are not yet available. We will discuss what is needed, especially in a federated environment, to avoid stovepipes with their negative side effects.

2.0 MULTI-DOMAIN SCENARIOS

In the following, we will describe two scenarios in which adversaries may run attacks in both the physical and cyber and information world to disturb an operation.

2.1 Host Nation Support

The first scenario is inspired by the Defender Europe 20 exercise. In a force deployment situation, the national territory serves for the transition of allied forces. On national territory, large scale coordination is required to support all troops during their transition. Beside other factors, resting places like a tent-based camp for thousands of US troops arriving by airplane, the transport of military equipment by rail and road as well as the escort for convoys have to be organized and monitored. As in real live in 2020, also the COVID-19 pandemic has its role in this scenario.

In this scenario, the staff responsible for planning and coordinating the host nation support mission has to deal with multiple events. Some of the main events are briefly described in the following.

Increasing COVID-19 infection rate: When Defender Europe 2020 was running, German infection law has foreseen a 14-day local lockdown if the infection rate rises above 50 new infections per 100,000 inhabitants within a given period of time. In the scenario, COVID-19 infection monitoring shows an increasing infection rate for one of the regions where US drivers have their resting place after coming in by airplane via Hamburg and before picking up their equipment that was shipped to Bremerhaven. By deviating to an alternative resting place, an unplanned 14-day quarantine for the US drivers could be avoided and with it a delay of the further transport of the equipment.

Cyber activities: The national cyber defence centre monitors activities that try to manipulate electronic traffic guidance systems within the scope of their responsibility of critical infrastructure monitoring. With early detection of these cyber activities, the mission planning staff is notified and closely interacts with the military police that is responsible for convoy escort. The military police operation centre tasks additional forces to deploy traffic guidance posts to the potentially affected roads. This allows for flexible local reactions in case of adversarial rerouting activities by manipulated electronic traffic guidance.

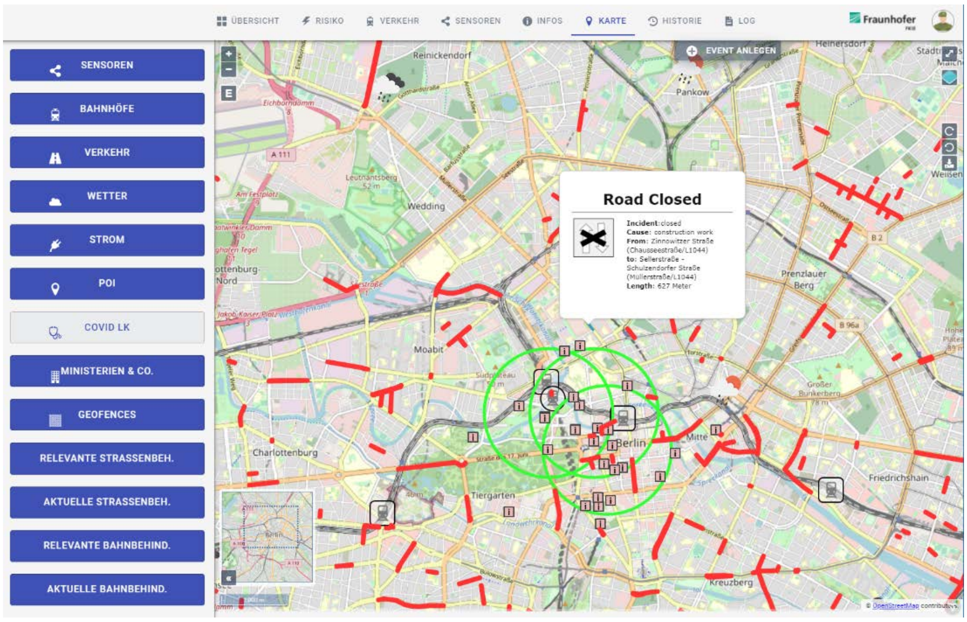
Activities of the civil population: By monitoring of social media and other channels, influencing of ‘environmental protection movements’ and other organised groups by information campaigns is detected. A detailed analysis shows that demonstrations and with it road blockings on main convoy routes are planned to delay the military equipment transportation. By defining indicators for the monitoring of the information domain as well as traffic jam information, the mission execution can react in a timely manner by measures like route deviation or an alternative rest stop at a nearby military base.

The main purpose of this scenario is to highlight the importance of monitoring multiple domains. Thus, information from very different sources comes together within the planning staff and has to be connected to estimate the effects on the own mission. The solution developed in our project demonstrates that connections between apparently unrelated events can be detected very early by bringing together all relevant information in a digital format, as well as supporting the full process of analysis and assessment up to mission briefings, decisions and deployment of measures in a digital way.

2.2 Territorial Operations

The second scenario is about a public swearing-in ceremony in front of the ‘Reichstag’ building in the government district of Berlin, Germany, like it took place in 2019. This scenario pronounces the challenges of an urban operation on own territory. In Germany, the civil authorities are responsible for public order. For that reason, the military mission planning has to cooperate very closely with the responsible civil actors. Additionally, the government district with multiple sensitive buildings is a critical area but publicly accessible. All in all, this brings in a lot of difficulties for military mission planning and execution. The solution developed in our project shows its support in integration, aggregation, and analysis of data as well as in generating a situational picture for detection and assessment of hybrid threats.

In this scenario, information for a specific area of operation come together from multiple sources, including information on energy supply, train and road traffic, incidents in train and road traffic, weather forecasts, critical buildings and other points of interest as well as data from locally deployed sensors and additional public sources.



Road Closed

Incident:closed
Cause: construction work
From: Zinnowitzer Straße (Chausseestraße/L1044)
to: Sellerstraße - Schulzendorfer Straße (Müllerstraße/L1044)
Length: 627 Meter

Figure 2-1: Map View of Situation Overview in Scenario 'Territorial Operations'

Mission planning staff is supported by bringing together the relevant information, aggregating it to a situation picture for regular briefings as well as decision support (see Figure 2-1). One of the challenging tasks is bringing together information from civil sources with own data from military sensors and additional data sources. During the planning phase of the operation, various events have to be assessed. Detection and tracking of a UAV by local sensors, multiple incidents in train traffic as well as public demonstrations against the military are examples of events that occur and require appropriate reactions.

3.0 HIGH-LEVEL ARCHITECTURE

In our project, a decision support system for mission planning has been developed that allows to detect and assess hybrid threats. The idea behind it is a flexible extendable suite of sensors and analysis modules, which generate information of relevant domains. The suite combines knowledge about physical movements, effects in the electromagnetic spectrum as well as actions in the cyber and information domain. This way, a comprehensive assessment of hybrid threats with respect to the mission planning is derived.

The benefit for the military users results from the comprehensive support for various participants in the planning and execution of a mission. Starting with edge processing of sensor data by the reconnaissance branch and the situational awareness assessment by the subject matter experts and analysts up to the combination of the data in a situational display – it all contributes to the overall situational awareness.

Figure 3-1 shows the high-level architecture of the decision support system. It assumes the following four types of threats:

- "Classic" military threats by means of physical presence

- Negative influence of the public opinion by spreading disinformation ("fake news") and causing reputational damage of the own troops and key persons
- Cyber attacks against military networks and critical infrastructures
- Impairing infrastructures like transportation (railways, roads) and utilities (energy, water, sewer)

For each of the categories, a number of exemplary sensors and components have been identified and implemented. They are described in more detail below. The aim is to derive actionable information from the various data sources, i.e., information that is meaningful and relevant within the context of a given mission. This information is presented to the user in an application for situational awareness and decision support.

Experience has shown that, despite support by artificial intelligence, actionable information cannot always be derived automatically from the sensors and information sources. It takes analysts / subject matter experts to conduct explorative data analyses (visual analytics) to, e.g., identify and evaluate trends in social media.

The general guideline of the approach is optimal support for the different user types and roles – without having a fully automated system. The amount of data and the complexity of detecting and assessing of hybrid threats can only be addressed with a suitable cooperation of human and machine.

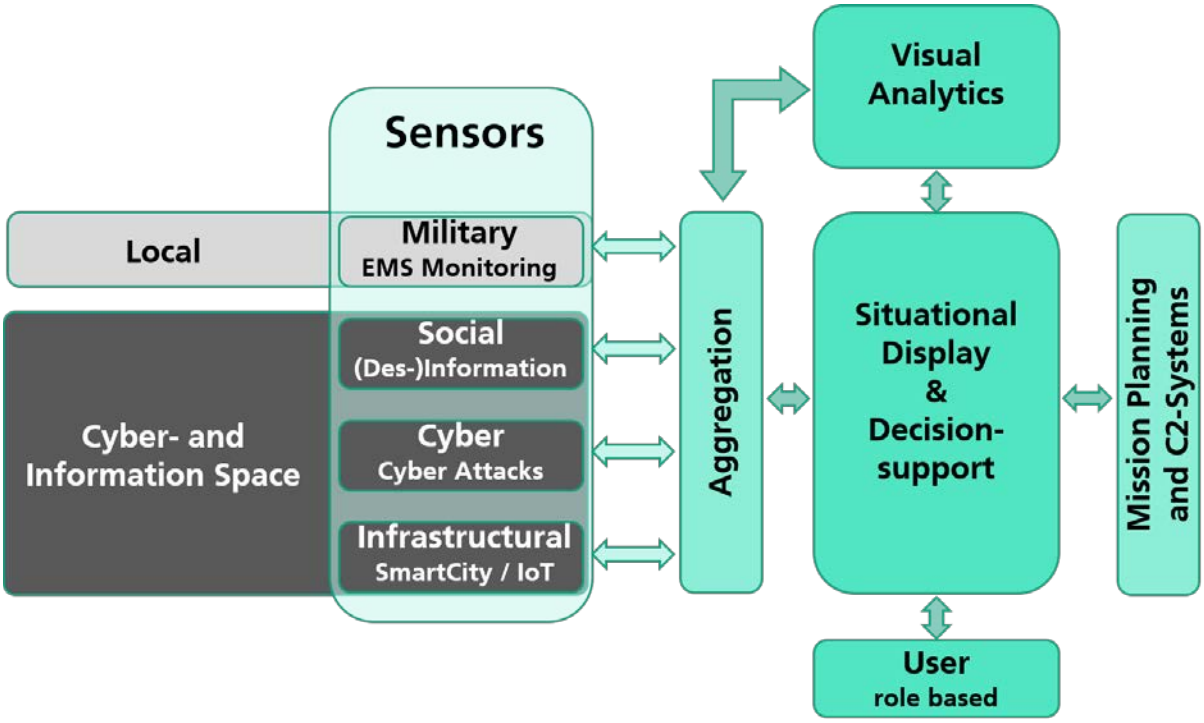


Figure 3-1: High-Level Architecture of the Demonstrator

4.0 SENSORS AND COMPONENTS

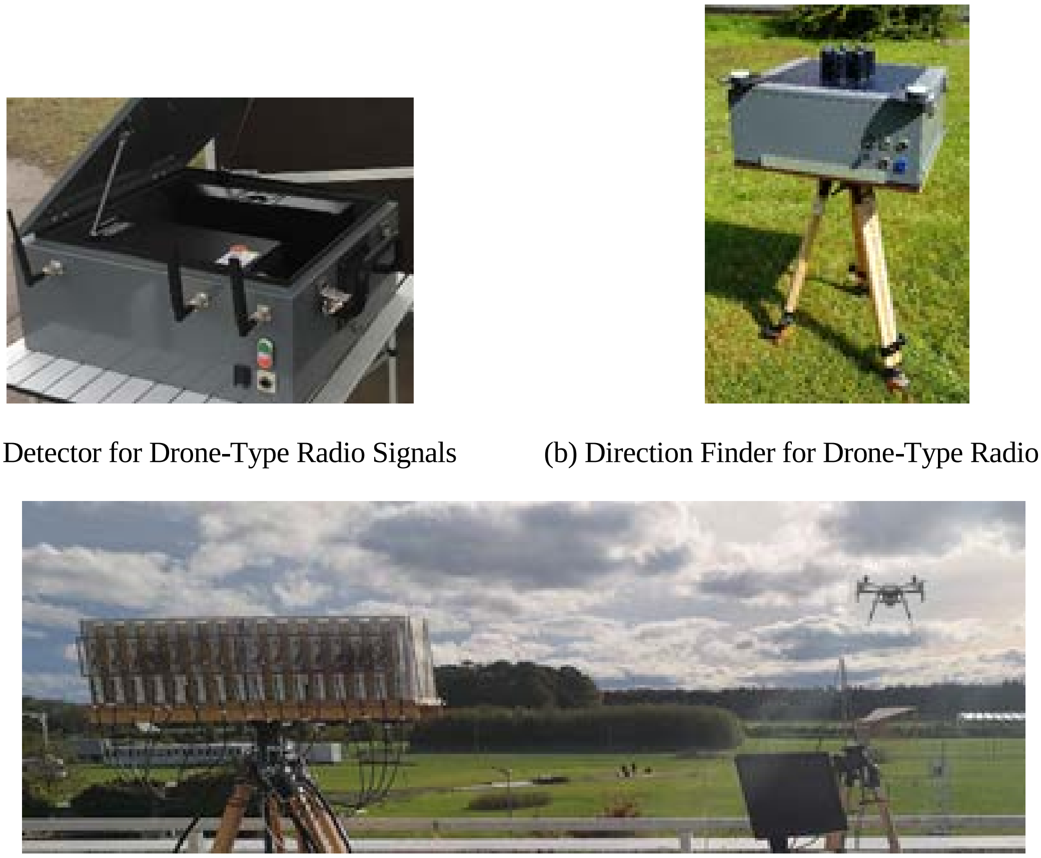
After showing the high-level architecture, the sensors and components of the demonstrator developed within the project are described below.

4.1 Classic Military Threats – Local Sensors

To sense classic type military threats, the respective sensors have to be in operation at the same time the actions to be detected take place. In addition, they must be placed at appropriate locations in order to be able to monitor the ongoing adverse actions. To emphasize the proper location as a crucial issue, we use the term *local sensors*.

Threats imposed by approaching drones were selected as example for classic military threats. Drones are considered as such unmanned aerial vehicles with a take-off gross weight of up to 5 kg (approx. 11 lbs). With respect to the ceremony scenario, an approaching drone may be considered as a threat, because it could be the carrier of CBRN (chemical, biological, radiological and nuclear) substances or gun type payloads – or it could be used for reconnaissance purposes in preparation of a later attack. For drone detection, local monitoring of the electromagnetic spectrum is a very effective means.

Several sensor systems have been integrated into our demonstrator. They are described below. Some hardware components are also shown in Figure 4-1.



(a) Detector for Drone-Type Radio Signals

(b) Direction Finder for Drone-Type Radio Signals

(c) Passive Radar for the Detection of Small Objects

Figure 4-1: Local Sensors

4.1.1 Detector for Drone-Type Radio Signals

Most of the drones considered are controlled using radio signals emitted by a remote control unit (RCU). These radio signals can be sensed in order to detect the presence of a drone and/or RCU within the detection range of the sensor. Our detector monitors the relevant bands (2.4 GHz) of the electromagnetic spectrum and recognizes drones and/or RCU radio signals due to their signal features. [1] [2] [3]

4.1.2 Direction Finder for Drone-Type Radio Signals

Following the detection of a drone-type radio signal, the bearing of these signals is determined by a direction finder. The result of this sensor enhances situational awareness by providing a direction in which a drone and/or a remote control unit has been detected.

4.1.3 Passive Radar

This sensor determines the location of a drone within its vicinity. A beneficial aspect of the use of this sensor in military theatres is its "passive" feature. Unlike most radar systems, it does not transmit any radio signals by itself. It rather uses the signals emitted by the base stations of cellular radio networks to locate the drones. When determining the position of a moving drone, the *Passive Radar* generates tracks of the flight path. These can be evaluated in order to discriminate between threat/no-threat for a given scenario. To enhance the validity of the tracks, the *Passive Radar* can be complemented by cameras for the detection of drones. Fusing the results of both components leads to more precise tracks. [4] [5] [6] [7] [8]

4.1.4 Jammer Detector

Using the same hardware as the *Detector for Drone-Type Radio Signals*, the *Jammer Detector* scans the electromagnetic spectrum for typical signals used by jammers. Opposing forces use jammers to interfere with the radio communication in order to make the attacked radio communication impossible or at least to degrade its use. In every day's situations, signals transmitted by jammers are not present. Thus, the detection of this type of signal is a strong indication for a beginning or ongoing adverse operation and, thus, contributes to the situational awareness. [1] [2] [3]

4.2 Threats using the Cyber and Information Domain – Remote Sensors

These sensors have access to data and information of their specific domain via the internet. They are tagged as *remote sensors*, because they do not require physical presence at a certain location.

4.2.1 Social Media Analysis

Nowadays, information as well as disinformation campaigns are mostly conducted using social media. The *Social Media Analysis* sensor has access to these media. It extracts messages and posts, which are selected by keywords or originators. Beyond the provision of the contents of these messages, the sensor allows for thorough analyses like "who-sends-certain-content" or "which-content-is-sent-by-whom". These analyses are supported by the *Visual Analytics* module, which is introduced later in this paper. The sensor focusses on text messages. Included links to audio information are forwarded to the sensor *Speech Reconnaissance*. Considering legal aspects when observing social media, the sensor monitors Twitter messages. [9] [10] [11] [12]

4.2.2 Speech Reconnaissance

A widely used means for influencing the public opinion is the spreading of spoken information in digital channels. These can be speech messages in social networks as well as clips in YouTube or reports broadcasted by radio or TV stations. The speech reconnaissance sensor implemented in the demonstrator can be fed with all kinds of digitized speech data. It is able to distinguish between speech and non-speech data and recognizes keywords, which are provided by the user. It can detect the language used in the analysed samples. Currently, this is implemented for German and English. The sensor also facilitates speaker recognition. This requires the provisioning of training data for the individual speaker.

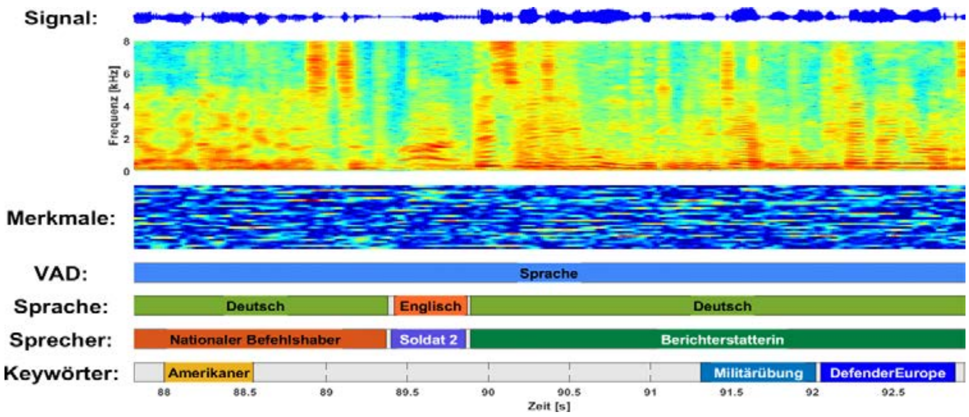


Figure 4-2: Speech Reconnaissance

In the demonstrator, this sensor is tasked by the *Social Media Analysis* sensor. Relevant messages extracted from social media frequently contain links to spoken posts. These links are forwarded to the speech recognition sensor, so that the content accessible via these links can be analysed. [13] [14] [15] [16] [17] [18]

4.2.3 Cyber Threat Intelligence

In the context of hybrid threat detection, knowledge regarding malicious operations within the cyber and information space on a global scale contributes to the full picture of risk assessment. Various governments as well as commercial companies provide reports describing launched attacks and the name of the respective attacker and the target. The sensor *Cyber Threat Intelligence* collects these reports and aggregates their content. Using explorative data analysis tools, the manifold of reported malicious operation can be analysed with respect to various dimensions.

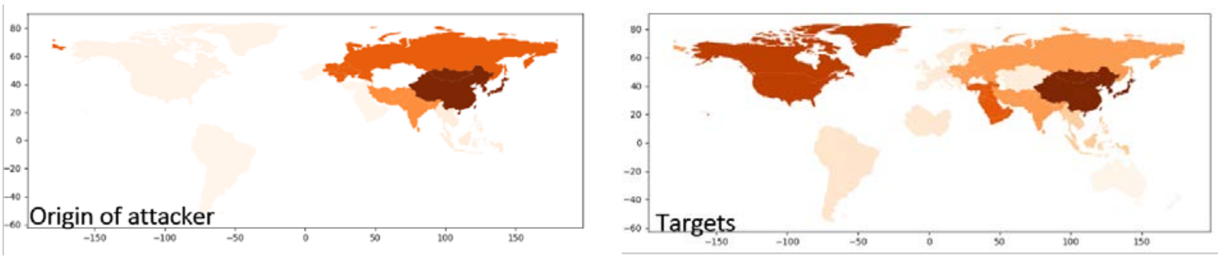


Figure 4-3: Cyber Threat Analysis

For further insight into this sensor, please see the paper "From Plain Text to CTI – A Technological Solution for Gathering Cyber Threat Intelligence using Natural Language Processing" of the IST-190 Symposium. [19]

4.2.4 Domain Name Service (DNS) Analysis

In the cyber and information domain, the appearance of new internet domains may point to adverse operations. Thus, newly appearing internet domains and their content are checked by the sensor *Domain Name Service Analysis*. Beside metadata like domain name, geo-references, and date of recognition, the actual content shared via this domain is considered. The content data is collected and filtered according to keywords provided by the user of the sensor. The results generated by this sensor are, for example, a value representing the current relevance of a given topic based on the number of new domains contributing to this topic. In addition, features such as geographical origin and the number of domains with malicious content give hints with respect to hybrid threats.

4.2.5 Open Data

There is a broad variety of open data that can be taken into account for mission planning. These data are gathered via sensors in the so-called Internet of Things (IoT) or shared as part of a Smart City strategy. They are provided by government agencies, local administrations, companies, or individuals. Depending on their source, they have different levels of trustworthiness. Information is available on the environment (e.g., weather forecasts), telecommunications (network availability, network disturbances), transport (train connections/railway networks, air traffic, shipping, and road traffic), health (air pollution, hospitals, pharmacies, illness cases/pandemics…), energy and water supply, and events (e.g., mass events such as demonstrations and sports events).

With respect to the scenario for a public swearing-in ceremony, we analysed data for train traffic and the energy infrastructure. By fusing information provided by public APIs of the *Deutsche Bahn* (*German Railroads*) and *OpenStreetMap*, we were able to track the current locations of individual trains and to determine delays and critical incidents (e.g., accidents). This may help to track the arrival of potential troublemakers at an early stage. Moreover, disruptions in the rail traffic within the area of operation can be analysed in near real-time.

The analysis of the energy infrastructure turned out to be challenging. While the status of the infrastructure of major network providers is known, municipal utilities do not deliver such information. For some missions, it may be useful, though, to know the status of the energy network down to the level of districts or streets. To overcome this limitation, we looked at charging stations whose status is provided by *OpenChargeMap*. If the number of failed charging stations within an area of interest exceeds a given threshold, this may indicate a general power outage.

4.3 Central Components

The central components of the solution for detection and assessment of hybrid threats are realized by a software framework of Fraunhofer FKIE that allows modular and flexible integration, processing, and visualisation of data. Sensors and data sources are integrated by a data integration layer and transformed into a common data model. After this step, the data from different sources is linked and aggregated in the data processing layer. The functionality of this layer can be enriched by data analytics capabilities based on Artificial Intelligence (AI) or Big Data Analytics. Here, the specific data aggregation and analytics functionalities depend on the data content, available historical data etc. In this layer, geo-specific analysis is also realised, enabling capabilities like the detection of tracked objects entering a geo fence. Finally, the visualisation is the part of the software that operators directly work with.

Operators can build up a situation picture based on their role-specific views. This way, subject matter experts like military police can, for example, focus on information that is relevant to them. Analysts that are responsible for building an overarching situation picture have broad access to more data sources according to their information needs. Regardless of views and filters used, all users operate on the same data, i.e., a common situation picture is given. For example, a military police domain expert may rate a threat of violent public protests as high with respect to a convoy mission. Then this information is directly available for the mission planning and execution staff. They can react instantly, e.g., by re-routing the convoy or sending protection forces.

As it is not always possible to foresee the information needs in such a complex information environment, visual analytics capabilities are an essential part of the solution. A system of automatic data aggregation, filtering, and assessment can be realised for some tasks based on indicators used by the subject matter experts or data analysts. But a technical system – nowadays and in the near future – will not be able to gain overall awareness of the situation and flexibly act in totally unforeseen situations. For working with a huge number of data sets that are analysed by an operator, the described solution uses a highly flexible dashboard. Subject matter experts can filter, aggregate, and link data on-the-fly for explorative data analytics with means of Visual Analytics. The resulting findings end up in detection and assessment of risks for mission planning and execution. They are documented within the system and thereby available for situation assessment and decision support.

The resulting situation picture, based on data aggregation and assessment, can be transferred to external systems, e.g., mission planning or command and control systems, but it can also be directly accessed by end users in the operation room or on a mobile device.

4.3.1 Aggregation

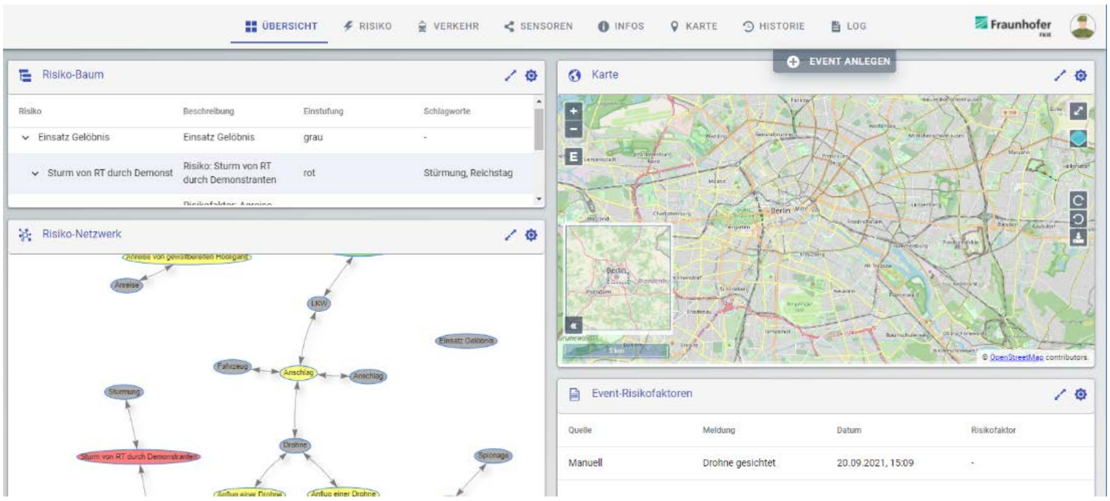
Data aggregation is happening on multiple levels. In many cases, the first aggregation will happen even before the data is integrated into the solution for hybrid threat detection and assessment. Current sensors pre-process data on their own hardware or provide specific analytics modules. This data pre-processing may even comprise a complex data fusion functionality that derives tracking information from multiple single sensor systems with different capabilities. The presented solution builds up on this and flexibly integrates raw data as well as pre-processed data.

As already described above, the data processing layer takes over after data integration. This layer contains modules for data analytics and aggregation. It is the place where higher level information is generated. In the demonstrator developed within the project, single sensor information like weather prediction information, current figures for COVID-19 infections, or tracking information from UAV detection are processed by separate microservices that provide the required level of linked data and aggregation. Hereby, the system is capable of monitoring, e.g., COVID-19 infection figures and link them to locations, which are relevant to the current situation assessment. Another example is an automatic warning if an unknown UAV enters a pre-defined area. Raw and aggregated data gets also tagged in this layer to enhance filter and warning capabilities for the operators.

Finally, the operator in front of the system is the instance doing the situation assessment by analysing the information, which is pre-processed and visualised by the system as supportive as possible.

4.3.2 Situational Display and Decision Support

The situational display and decision support functionality builds on the data processing layer and its data analytics and integration capabilities described above. The role-specific user interface is web-based and consists of a manifold of different views through which the operator can navigate (see Figure 4-4). Each view has sub-elements that are displayed in a responsive design, i.e., they adapt to different display sizes and resolutions automatically.



Risiko-Baum

Risiko	Beschreibung	Einstufung	Schlagworte
Einsatz Gelöbnis	Einsatz Gelöbnis	grau	-
Sturm von RT durch Demonst	Risiko: Sturm von RT durch Demonstranten	rot	Stürmung, Reichstag

Event-Risikofaktoren

Quelle	Meldung	Datum	Risikofaktor
Manuell	Drohne gesichtet	20.09.2021, 15:09	-

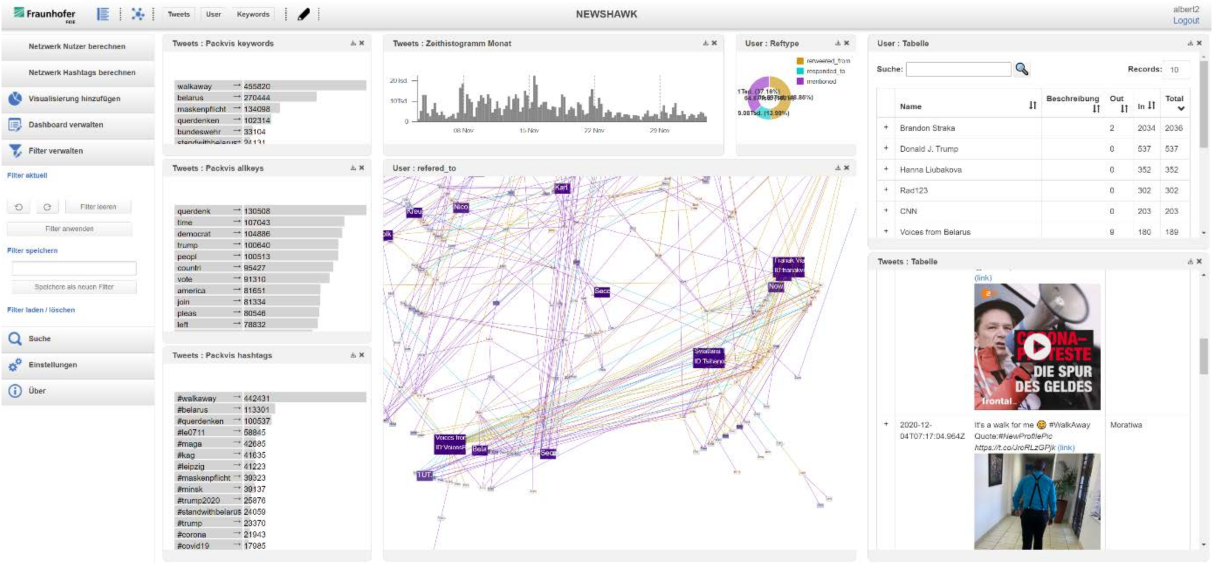
Figure 4-4: Situational Display

Switching between the different views on the top, the operator gets the data from the different sensors and data sources that was aggregated and pre-processed for his purposes in the specific visualisation and interaction elements. These may be simple tables that enable sorting and filtering, but also a graph visualisation, diagrams, or a map that contains different overlays. For example, a view for visualisation of infrastructure may contain a map that shows the power supply status for a city in one layer and the railway infrastructure status in another layer. A second module in the same view may be a table that shows the traffic jams on the road, sorted by length. Each module of a view serves a specific purpose. The modules are joined together to form the suiting views per role when the system is set up for the different user types.

The most important user interface element is one that can be faded in at the top on every view. It contains the risks for hybrid threats that were already identified. Based on the information of each view, the operator documents his assessment of the situation by adding or editing risk factors. Each risk factor may be connected to multiple risks. So, experts for multiple domains can do their individual assessment within their specific views in parallel while the analyst being responsible for the overarching situation picture gets their updates in real-time and does his/her overall risk assessment based on this information.

4.3.3 Visual Analytics

In order to recognize correlations and relationships within sensor data, a component for visual analytics has been integrated into the demonstrator (see Figures 4-5 and 4-6). Using dash boards allows for a very versatile visualization of the sensor data. *Visual Analytics* is applied very beneficially for the exploration of data that describes information flows from originators with specific content to recipients. By setting the correct parameters, the visualization reveals correlations and relationships within the data. The knowledge about these connections can be implemented into the aggregation schemes for the sensor data. Thus, the determination of the risk coming from the threats in view becomes more reliable.



walkaway	455820
belarus	270444
maskenpflicht	134098
querdenken	102314
bundeswehr	33104
standwithbelarus	24131

querdenk	130508
time	107043
democrat	104886
trump	100640
peopl	100513
countri	95427
vote	91310
america	81651
join	81334
pleas	80546
left	78832

#walkaway	442431
#belarus	113301
#querdenken	100537
#le0711	58845
#maga	42685
#kag	41635
#leipzig	41223
#maskenpflicht	39323
#minsk	39137
#trump2020	25876
#standwithbelarus	24059
#trump	23370
#corona	21943
#covid19	17985

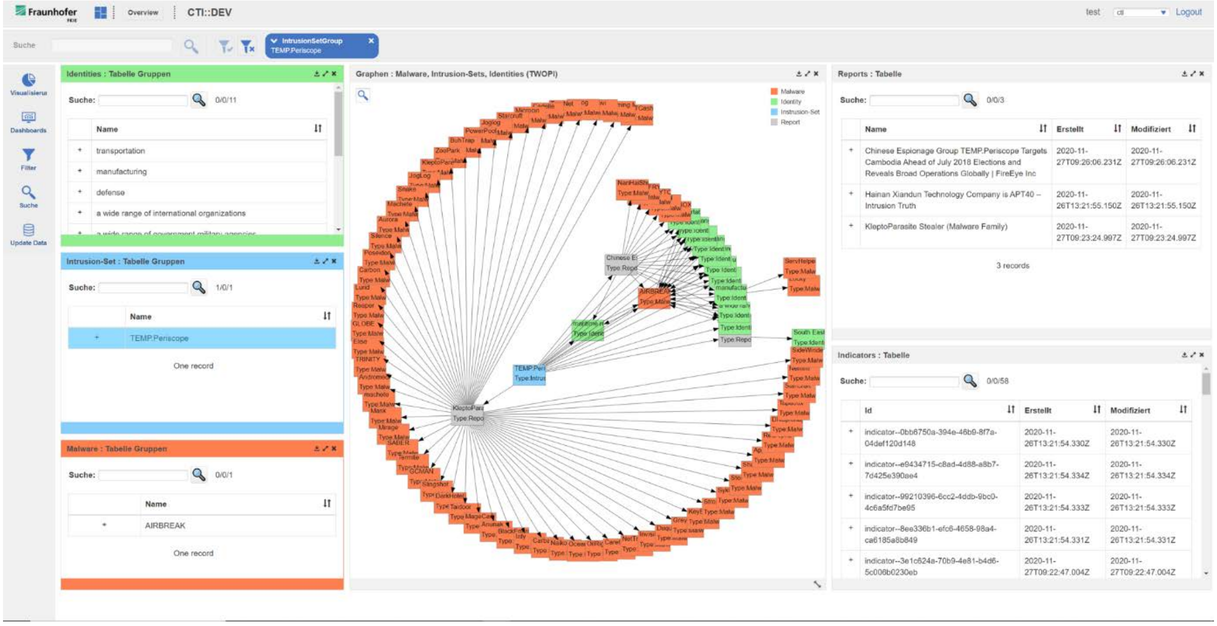
User : Tabelle

Suche: Records: 10

	Name	Beschreibung	Out	In	Total
+	Brandon Straka		2	2034	2036
+	Donald J. Trump		0	537	537
+	Hanna Liubakova		0	352	352
+	Rad123		0	302	302
+	CNN		0	203	203
+	Voices from Belarus		9	180	189

+	2020-12-04T07:17:04.964Z	It's a walk for me 😊 #WalkAway Quote:#NewProfilePic *https://t.co/JrcRLzGPjk* (link)	Moratiwa

Figure 4-5: Visual Analytics – Dashboard for Explorative Social Media Analysis



Identities : Tabelle Gruppen

Suche: 0/0/11

	Name
+	transportation
+	manufacturing
+	defense
+	a wide range of international organizations
+	a wide range of government military agencies

Intrusion-Set : Tabelle Gruppen

Suche: 1/0/1

	Name
+	TEMP.Periscope

One record

Malware : Tabelle Gruppen

Suche: 0/0/1

	Name
+	AIRBREAK

One record

Reports : Tabelle

Suche: 0/0/3

	Name	Erstellt	Modifiziert
+	Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally | FireEye Inc	2020-11-27T09:26:06.231Z	2020-11-27T09:26:06.231Z
+	Hainan Xiandun Technology Company is APT40 – Intrusion Truth	2020-11-26T13:21:55.150Z	2020-11-26T13:21:55.150Z
+	KleptoParasite Stealer (Malware Family)	2020-11-27T09:23:24.997Z	2020-11-27T09:23:24.997Z

3 records

Indicators : Tabelle

Suche: 0/0/58

	Id	Erstellt	Modifiziert
+	indicator--0bb6750a-394e-46b9-8f7a-04def120d148	2020-11-26T13:21:54.330Z	2020-11-26T13:21:54.330Z
+	indicator--e9434715-c8ad-4d88-a8b7-7d425e390ae4	2020-11-26T13:21:54.334Z	2020-11-26T13:21:54.334Z
+	indicator--99210396-6cc2-4ddb-9bc0-4c6a5fd7be95	2020-11-26T13:21:54.333Z	2020-11-26T13:21:54.333Z
+	indicator--8ee336b1-efc6-4658-98a4-ca6185a8b849	2020-11-26T13:21:54.331Z	2020-11-26T13:21:54.331Z
+	indicator--3e1c624a-70b9-4e81-b4d6-5c006b0230eb	2020-11-27T09:22:47.004Z	2020-11-27T09:22:47.004Z

Figure 4-6: Visual Analytics –
Dashboard for Explorative Data Analysis for Cyber Threat Intelligence

4.3.4 External Interfaces

The demonstrator is intended to be used for mission planning and during the execution of a mission. Mission planning is always done in an office-type environment with the user operating at his/her terminal. Monitoring of an ongoing mission is mostly done at the same position and may additionally be done by mobile devices. If, e.g., personnel of the military police is involved during the action – for instance, when guiding military convoys over the roads – they can work with smart phones or tablets. These will be connected to the servers hosting the situational display. The features of the devices are designed role-based, so that, depending on the particular role of the user, the proper information is provided.

The demonstrator and the resulting product will be deployed within an existing environment for mission planning as well as mission execution. Thus, an integration with existing systems is necessary. Data distribution to operational level mission planning systems as well as command and control (C2) systems is part of the concept. The information exchange will be handled via provided interfaces.

5.0 CHALLENGES OF CONNECTING THE DOTS

A key challenge of tackling hybrid threats is the diversity of data sources and tools supporting their analyses. The types of components range from sensors that emit status messages and alerts to highly complex processing systems. Data may be provided as machine-processable messages with a clear syntax and semantics or as free-text documents. Quite often the analysis is performed by subject matter experts that summarize their findings in status reports.

To cope with hybrid threats, information exchange across multiple domains is needed. The authors are not aware of any military standard that facilitates the exchange between the land, maritime, air, and space domain on the one hand and the cyber and information domain on the other hand. Standards such as the *MIP 4 Information Exchange Specification* (*MIP4-IES*) support the physical space pretty well but lack concepts from the cyber space. Edition E of *APP-6 NATO Joint Military Symbology* is expected to standardize cyber symbols and to facilitate their exchange but they are defined as individual symbols without links to other concepts.

It is also not entirely clear what level of abstraction would be suitable for cross-domain information exchange, because this depends on requirements of the specific environment to be supported. In any case, though, traceability to the original (raw) data must be preserved. For instance, when inferring real-world incidents – which are displayed on a map – from social media reports, it must be possible for the operator to drill down to the original statements that were published.

6.0 SUMMARY & OUTLOOK

The demonstrator presented in this paper is based on a modular concept. The objective was to build up the continuous and digital data processing chain from multiple sensors and data sources via data analytics to the user interface. To reach this objective, it was an obvious choice to rely on FKIE in-house sensors in a first step. The first demonstrations ran successfully and proved the feasibility of the chosen approach. A highly significant point is the underlying concept. It is designed to add other sensors and data sources as well as analytics services and visualisation modules. This is a fundamental requirement for providing a future-proof solution. New sensors and data sources from different vendors will come up with new technologies as well as new data analytics methods, frameworks, and hardware devices for visualisation.

The current research project is running until end of April 2022. Within the project, the next steps are the integration of additional sensors and evaluation sessions with potential users within the communities of interest to get feedback and improve the concept and demonstrator. After this proof of concept in the current project, the results will be presented to military and civil stakeholders that deal with the detection and assessment of hybrid threats. For a proof of concept in real-world situations, a long-term evaluation would be the means of choice. With the increasing number of aggregated data in digitalised formats, the use of advanced data science methods will also be possible on higher levels of abstraction. This will bring in additional support to operators and is an important enabler for situational awareness and decision support in highly dynamic operation environments.

REFERENCES

[1] F. Kurth, H.-G. Lehn, R. Parting, "Verfahren zur Erkennung eines oder mehrerer Nutzsignale innerhalb eines Quellsignals", Deutsches Patent DE 10 2009 035 524, 2009.

[2] S. Kreuzer, R. Peter, A. Höck, „Effiziente Funksignaldetektion in Breitbandaufzeichnungen mit findus“, FKIE Jahresbericht, 2013.

[3] S. Urrigshardt, S. Kreuzer, F. Kurth, "Signalanalyse, Detektion und Klassifikation mit dem findus2-Analysator", FKIE Jahresbericht 2020.

[4] C. Steffes, B. Demissie, B. Knödler, M. Brötje, M. Mandt, W. Koch: „Passive Radar using Mobile Communication: A Discussion of Use Cases and Feasibility“, RadarConf2022.

[5] B. Knoedler, C. Steffes, W. Koch, ‘Detecting and Tracking a Small UAV in GSM Passive Radar Using Track-before-Detect,” 2020 IEEE Radar Conference (RadarConf20), Florence, Italy, Sept 2020.

[6] B. Knoedler, R. Zemmari, W. Koch, “On the detection of small UAV using a GSM passive coherent location system,” 17th International Radar Symposium IRS 2016, Krakow, Poland, May 2016.

[7] S. Jovanoska, M. Broetje, W. Koch, ”Multisensor Data Fusion for UAV Detection”, 19th International Radar Symposium IRS 2019, Bonn, Germany, June 2021.

[8] S. Jovanoska, B. Knoedler, D. Palur Palanivelu, L. Still, M. Varela, T. Fiolka, M. Oispuu, C. Steffes and W. Koch, “Passive Sensor Processing and Data Fusion for Drone Detection,” NATO STO Meeting Proceedings: MSG-SET-183 Specialists’ Meeting on Drone Detectability: Modelling the Relevant Signature, July 2021.

[9] Schade, U., Meißner, F., Pritzkau, A. & Verschitz, S., “Prebunking als Möglichkeit zur Resilienzsteigerung gegenüber Falschinformationen in Online-Medien", in Zowislo-Grünewald, N. & Wörmer, N. (Hrsg.), Kommunikation, Resilienz und Sicherheit (pp. 134-155). Berlin: Konrad-Adenauer-Stiftung, 2021.

[10] Winkelholz, C. & Schade, U., “NewsHawk zur Lagefeststellung – Beobachten und Analysieren im öffentlichen Informationsraum” in Crisis Prevention, 3/2020, 62-64, 2020.

[11] Pritzkau, A. & Schade, U., “Vorsicht: mögliche „Fake News“ – ein technischer Ansatz zur frühen Erkennung” in: Klimczak, P. & Zoglauer, T. (Hrsg.), Wahrheit und Fake im postfaktisch-digitalen Zeitalter. Distinktionen in den Geistes- und IT-Wissenschaften. Wiesbaden: Springer-Vieweg, 2020.

[12] Pritzkau, A., Schade, U., Claeser, D. & Winandy, S., Projekt „Narrativ“ – Projektabschlussbericht. Wachtberg: Fraunhofer FKIE, 2020.

[13] D. Von Zeddelmann, F. Kurth, M. Müller, Perceptual audio features for unsupervised keyphrase detection, in International Conference on Acoustics, Speech and Signal Processing (ICASSP), S. 257–260, IEEE, 2010.

[14] P. Baggenstoss, F. Kurth, "Robuste Sprechersegmentierung und –identifikation (ROSIE)", Projektbericht FKIE 2017.

[15] K. Wilkinghoff, A. Cornaggia-Urrigshardt, F. Gökgöz, “Two-Dimensional Embeddings for Low-Resource Keyword Spotting Based on Dynamic Time Warping” in 14th ITG Conference on Speech Communication, 9-13.

[16] Kevin Wilkinghoff “On Open-Set Speaker Identification with I-Vectors”, in: Odyssey - The Speaker and Language Recognition Workshop (Odyssey). ISCA, 2020, pp. 408–414.

[17] Kurth, Frank, Alessia Cornaggia-Urrigshardt, Sebastian Urrigshardt. "Robust F0 estimation in noisy speech signals using shift autocorrelation." In 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2014.

[18] F. Kurth, A. Cornaggia-Urrigshardt, A. Höck, and R. Kamlage, “Vorrichtung und Verfahren zur Detektion und Klassifikation von Sprachsignalen innerhalb breitbandiger Quellsignale.” Deutsches Patent, 2015.

[19] R. Müller, "From Plain Text to CTI – A Technological Solution for Gathering Cyber Threat Intelligence using Natural Language Processing" in IST-190 Research Symposium (RSY) on AI, ML and BD for Hybrid Military Operations (AI4HMO).