DITS.center e.V.

Positionspapier Sicherheits-forschung

DITS äußert sich gemeinsam mit Experten
zu den Fragen einer zukünftigen Gestaltung
von BMBF Förderprogrammen.

Anwender können gemeinsam
mit motivierten Unternehmen
und Forschungseinrichtungen
Innovationen schaffen,

die der zivilen Sicherheit in der Gesellschaft dienen
sowie wirtschaftliches Wachstum
in einem interessanten globalen Markt begründen.

SiFo
2022

Inhaltsverzeichnis

1	Einführung	2
2	Rahmenbedingungen	3
2.1	Innovationstreiber – Anwender und Rollenverteilung	3
2.2	Innovationstreiber – Startups, Scaleups und KMUs	4
2.3	Innovationstreiber – Forschungseinrichtung	5
2.4	Innovationstreiber – Senior-Experte	6
2.5	Internationale Zusammenarbeit mit der Ukraine	7
3	Projektvorschläge	8
3.1	Vorbemerkungen	8
3.2	Monitoring sozialer Medien	9
3.3	Lieferkettensorgfaltspflichtengesetz (LKSG)	10
3.4	Aspekte zum Datenschutz – Löschen und Qualitätsmanagement	12
3.5	DITS – diverse Projektvorschläge	14

1 Einführung

Es besteht kein Zweifel daran, dass BMBF Förderprogramme nachhaltigen Einfluss auf die Forschung, die Industrie und die Anwender haben und sich positiv auf die Steigerung der Fähigkeiten im Bereich der zivilen Sicherheit auswirken. Insbesondere erfüllen die Programme den Anspruch auf relativ überschaubare und unbürokratische Begleitprozesse für alle Beteiligten.

Das BMBF beabsichtigt die Fortschreibung des Rahmenprogramms **„Forschung für die zivile Sicherheit“** in dem sich auch DITS gemeinsam mit seinen Mitgliedern mit Anträgen auf Förderung erfolgreich engagiert hatten [Link] [DITS]. Die Einladung des BMBF richtet sich an alle Interessierten und Engagierten in der Gesellschaft:

„Die Folgen des Klimawandels, der technologische Fortschritt, tiefgreifende gesellschaftliche Veränderungen und nicht zuletzt aktuelle Entwicklungen wie die Corona-Pandemie oder der Krieg in der Ukraine werden die zivile Sicherheitsforschung in den kommenden Jahren vor neue und anspruchsvolle Herausforderungen stellen. Das BMBF führt deshalb einen Agendaprozess durch, um das Rahmenprogramm „Forschung für die zivile Sicherheit“ über das Jahr 2023 hinaus fortzuschreiben. Expertinnen und Experten aus Forschung, Wirtschaft und Anwenderkreisen, aber auch interessierte Bürgerinnen und Bürger können sich dabei aktiv mit ihren Bedarfen, Ideen und Themen einbringen.“

DITS engagiert sich als gemeinnütziger Verein seit 2016 im Bereich der Förderung von Wissenschaft und Forschung (§ 52 Abs. 2 Satz 1 Nr. 1 AO) sowie der Förderung der Volks- und Berufsbildung (§ 52 Abs. 2 Satz 1 Nr. 7 AO).

Erfahrungen aus Initiativen, Projekten und dem Netzwerk von Experten, Anwendern, der Industrie mit dem Schwerpunkt auf KMUs, Anwendern und Forschungseinrichtungen mündeten in den hier eingebrachten Beiträgen.

Autorenbeiträge sind unverändert und ungekürzt wiedergegeben.

DITS und alle Autoren freuen sich über Rückmeldungen bzw. Diskussionen.

2 Rahmenbedingungen

2.1 Innovationstreiber – Anwender und Rollenverteilung

2.1.1 Kurzfassung

Innovationen decken per se einen **konkreten** Bedarf. Nur die Anwendung schafft **Marktpotenzial**. Treiber für einschlägige Projekte müssen daher zuallererst der Anwender und ein marktorientiertes Unternehmen sein. Forschung dient dem Anwender sowie dem Unternehmen und schließt Fähigkeitslücken im Bereich von Technologien und ggf. auch in der Begleitung der späteren Verwendung.

2.1.2 Themenfeld

Eine **Innovation** ist das Ergebnis der Entwicklung und Überführung einer Idee oder Erfindung in ein Produkt, einen Service oder Prozess. Eine Innovation muss zu ökonomischen Kosten replizierbar sein und einen spezifischen Bedarf decken. Die Innovation schafft Werte oder der Kunde ist bereit, dafür zu bezahlen.

Forschung muss vom **Bedarf**, den **Fähigkeitslücken** bei den Anwendern und der **Initiative** innovativ geprägter Unternehmen getrieben werden.

Zitat aus [BMBF, 2022]: *„Exzellente Forschungsergebnisse kennzeichnen das deutsche Forschungs- und Innovationssystem. Sie schaffen eine breite Wissensbasis, werden aber vielfach noch nicht weitreichend genug genutzt oder finden noch zu langsam ihren Weg in die Anwendung.“*

Es ist eine Mär, dass Technologietransfer eine Einbahnstraße von der Forschung in Richtung des Nutzers von Forschungsergebnissen sei. Vielmehr bedeutet jedes Gemeinschaftsprojekt den gegenseitigen **Austausch auf Augenhöhe** von Erfahrungen, Erkenntnissen und auch von wissenschaftlichen Ergebnissen.

Die im Bundesbericht dargestellte Problematik ist seit langem bekannt und wird sich nur dann ändern, wenn die **Rollenverteilung** verändert wird. Es sind nicht die Forschungsergebnisse, welche Anwender, Gründer und Unternehmen motivieren (technology push). Vielmehr muss exzellente anwendungsorientierte Forschung dem spezifischen Innovationsprojekt dienen (**market pull**).

Anwender werden in den Rahmenbedingungen „Anwender-Innovativ“ trefflich benannt [BMBF AnwInno, 2018]. Hinzu kommen einschlägige Organisationen und auch Industrien.

2.1.3 Handlungsempfehlungen

Die Rolle der Anwender muss für Unternehmen und die Forschungseinrichtungen entwickelt und nachhaltig erschlossen werden.

Sicherheitsbehörden sollten geeignet ermuntert werden, die Chancen und Möglichkeiten passender Forschungsvorhaben zu nutzen. Neben dem unmittelbaren Nutzen sowie geringen Kosten dienen Projekte der Weiterbildung und der Motivation der damit befassten Mitarbeiter.

Senior-Experten [siehe 2.4 Innovationstreiber – Senior-Experte] können maßgeblich dazu beitragen, Anwender, Unternehmen und Forschungseinrichtungen in einem erfolgreichen Team zu verknüpfen.

2.1.4 Literatur

[BMBF AnwInno, 2018]: Anwender - Innovativ: Forschung für die zivile Sicherheit, https://www.bmbf.de/bmbf/shareddocs/bekanntmachungen/de/2018/04/1702_bekanntmachung.html.

[BMBF, 2022]: Bundesbericht Forschung und Innovation 2022.

2.2 Innovationstreiber – Startups, Scaleups und KMUs

2.2.1 Kurzfassung

Das Potenzial von **Startups** und **Scaleups** bei der Schaffung von Innovationen gilt als gewaltig, was zum Beispiel in Studien von Roland Berger mit Nachdruck vertreten wird [RolBerger, 2018], [RolBerger, 2021]. Die bestehende Offenheit, auch junge, durchfinanzierte Unternehmen zu fördern, wird begrüßt und soll weiter erhalten werden.

2.2.2 Themenfeld

Innovatoren benötigen drei Eigenschaften: realistische Einschätzung von Situationen, Hartnäckigkeit ein Ziel zu verfolgen und den starken Willen, neue Ideen und Lösungen zuzulassen. Es ist heute unstrittig, dass große Organisationen, die von verbindlichen Prozessen, Budgets und einem EBIT-bezogenen Berichtswesen beherrscht werden, Schwierigkeiten haben, die Schöpfer vielversprechender Ideen angemessen zu unterstützen. Das Tagesgeschäft erlaubt es häufig nicht, dass die "zarten Triebe" der Innovation wachsen. Wertvolle Ideen gehen im Tagesgeschäft verloren.

Es erfordert besondere Aufmerksamkeit sowie eine Atmosphäre von Freiheit, Vertrauen, Offenheit und kooperativen Verhaltens zur Förderung innovativer Teams.

Die Bereitschaft, sich auf Neues einzulassen und nicht zuletzt auch Risiken einzugehen, ist insbesondere bei **jungen Unternehmen** mit ihren **Gründern** und **Mitarbeitern** zu finden.

Start-Ups im Allgemeinen und die motivierten Unternehmer im Besonderen sind fähig, diese Rahmenbedingungen zu schaffen und nachhaltig zu erhalten.

Zu berücksichtigen ist, dass insbesondere die hier interessanten Start-Ups in der Regel über eine gesicherte Finanzierung und auch die Begleitung von Business-Angels als wesentliches Element der zielgerichteten Unternehmensentwicklung verfügen. Diese Bedingungen rechtfertigen Vertrauen auch in die jungen Unternehmen mit ihren besonderen Fähigkeiten.

2.2.3 Handlungsempfehlungen

Nur in Verbindung mit einem innovationsbereiten Unternehmen ist es möglich, Innovationen zu schaffen. Folgerichtig muss das **Duo Anwender & Unternehmen** die Projektinitiative begründen. Es lohnt sich in vielerlei Beziehung insbesondere das Engagement der Startups, Scaleups und KMUs zu fördern und in den Mittelpunkt der Strategien zu stellen.

Die Ermittlung der förderfähigen Kosten sollte überdacht werden. Beispiel: entsprechend der Erläuterungen „Anwender Innovativ“ wird der Stundensatz des Unternehmens unter Berücksichtigung von 2.080 Arbeitsstunden pro Jahr berücksichtigt (incl. Urlaub) – abgerechnet werden jedoch nur die tatsächlich geleisteten Arbeitsstunden; dies schafft defakto eine Kürzung der Förderquote.

2.2.4 Literatur

[RolBerger, 2021]: Pressemitteilung, Für ein Wirtschaftswunder 2.0: Neue Studie zeigt beeindruckende Beschäftigungseffekte von Startups und Scaleups auf den deutschen Arbeitsmarkt, https://www.presseportal.de/pm/32053/4949304.

[RolBerger, 2018]: Roland Berger, Start-ups sind die wichtigsten Innovatoren für Künstliche Intelligenz – Europa muss Rahmenbedingungen schaffen, um wettbewerbsfähig zu bleiben, https://www.presseportal.de/pm/32053/3945899.

2.3 Innovationstreiber – Forschungseinrichtung

2.3.1 Kurzfassung

Forschungseinrichtungen sind bestens aufgestellt, **Fähigkeitslücken** in Forschungs- und Entwicklungsprojekten zu schließen. Die Partnerschaft in **Arbeitsgemeinschaften** muss auf Augenhöhe aller Beteiligter gestaltet werden. Fragen zu gegenseitigen **Nutzungsrechten** müssen frühzeitig, fair und angemessen für alle Beteiligten geregelt werden.

2.3.2 Themenfeld

Ein erfolgreiches Gemeinschaftsprojekt gelingt nur dann, wenn die Interessen aller Beteiligter in **fairer** Weise berücksichtigt und gewahrt werden sowie ein gemeinsames Ziel definiert ist. Neben technisch-wissenschaftlichen Aspekten müssen die Partner für ein überzeugendes und belastbares **Projektmodell** sorgen. Alle Beiträge müssen zusammenwirken und dürfen nicht unabhängig voneinander nur zum Zweck der Gewinnung der Förderung aufgestellt werden.

Forschungseinrichtungen finanzieren sich in der Regel aus der Grundfinanzierung, Finanzierung aus Aufträgen der Wirtschaft sowie öffentlicher Projektfinanzierung. Forschungseinrichtungen genießen ein hohes Ansehen und gelten als wesentliches Element in Innovationsprozessen. Die Ausstattung und die Ressourcen der Einrichtungen sind **bestens** geeignet, technologische Lücken in Entwicklungsvorhaben auf **hohem Niveau** zu schließen. Gemeinnützige Organisationen verfolgen keine finanziellen Gewinnziele.

Trotz dieser Rahmenbedingungen bestehen bei der Industrie und den Anwendern **Ressentiments** im Hinblick auf projektbezogene Partnerschaften. Teils mögen diese auf Vorurteilen basieren, teils sind die Bedenken gerechtfertigt und basieren auf Erfahrungen. In jedem Fall begründet diese Zurückhaltung die beklagte unzureichende Überführung exzellenter Forschungsergebnisse in Innovationen.

Die Verwertung der Forschungsergebnisse wird unter Umständen durch **Schutzbedürfnisse** der Forschungseinrichtungen behindert, deren Berechtigung und Reichweite im Einzelfall durchaus in Frage gestellt werden können.

Anwender und kleinere Unternehmen verfügen in der Regel nicht über solche **juristische Ressourcen**, die sich in Forschungseinrichtungen mit der Gestaltung von Kooperationsverträgen auseinandersetzen.

2.3.3 Handlungsempfehlungen

Vollständig geförderte bzw. durch Drittmittel finanzierte Forschung gemeinnütziger Einrichtungen muss einer **freizügigen** Nutzung zur Verfügung stehen. Übertriebene Einschränkungen schrecken ab und wirken kontraproduktiv.

Anwender und insbesondere innovationsbereite KMUs müssen ermuntert werden, Projektskizzen, Anträge und Kooperationsverträge in **eigener Initiative** maßgeblich zu gestalten. Forscher oder Agenturen können diese Rolle nicht als Ghostwriter übernehmen. Die Authentizität der Ausführungen, konkrete und belastbare Hinweise auf die vorgesehene wirtschaftliche Verwendung und die Initiative der Nutzer müssen wesentliche Auswahlkriterien in der Projektförderung werden. „Anwender Innovativ“ bietet einen guten Ansatz.

Die bestehenden Hemmnisse und auch die prozessbedingten Erschwernisse für Anwender und junge Unternehmen in der Ausgestaltung von Kooperationsverträgen müssen gemindert werden. Verbindliche **Musterelemente** für Verträge wären zielführend.

2.3.4 Literatur

[FHG, Fin] Finanzierung der Fraunhofer-Gesellschaft, https://www.fraunhofer.de/de/ueber-fraunhofer/profil-struktur/zahlen-und-fakten/finanzen.html .

[Walter, 2002]: Achim Walter: Technologietransfer zwischen Wissenschaft und Wirtschaft – Voraussetzungen für den Erfolg, Habilitationsschrift TU Berlin.

2.4 Innovationstreiber – Senior-Experte

2.4.1 Kurzfassung

Wissen, Erfahrungen, Ideen und die Fähigkeiten unabhängiger und neutraler Experten können insbesondere im interdisziplinären Umfeld der sicherheitsorientierten Forschung wesentliche und beste Beiträge im Projektverlauf liefern. Neben assoziierten Partnern wird vorgeschlagen, den **Senior-Experten** als optionalen Projektpartner vorzusehen.

2.4.2 Themenfeld

Projektteams können durch Assoziierte Partner ergänzt werden. Im Bereich der Sicherheitsforschung ist dieser Begriff allerdings nicht definiert. In anderen Förderszenarien wird der Assoziierte Partner z.B. wie folgt beschrieben: *„Assoziierte Partner tragen ohne Förderung beispielsweise mit finanziellen, infrastrukturellen oder inhaltlichen (Personal-)Leistungen zum Projekt bei“.*

Die bestehenden **Beratungsangebote** durch den **Projektträger** und auch die **Förderberatung** des Bundes sind wesentliche Elemente im Projektverlauf. Zusätzlich kann insbesondere im Bereich der Sicherheitsforschung ein erfahrener Senior-Experte wesentliche Beiträge zum Gelingen und Erfolg eines Forschungsprojekts leisten.

Unabhängige Senior-Experten mit einschlägigen und langjährigen Erfahrungen sind fähig, Teambildung, Projektfokus, Marktrelevant und auch die Projektmoderation zu fördern. Wissen, Erfahrung, Netzwerke, hohe Professionalität und kurze Einarbeitungszeiten helfen in allen Phasen des Projektverlaufs. **Mitwirkung** in den Bereichen Einsatz, Forschung und Technologie, Recht, Unternehmensführung und Marktzugang, Empathie und eine entspannte Einstellung im Kreis aller Interessensvertreter unterstützt in komplexen interdisziplinären Projektszenarien, den richtigen Weg auch in komplizierten Situationen zu finden.

Insbesondere bieten **Führungskräfte im Ruhestand** ihre Mitwirkung an, und sind hochmotiviert fähig, sich im erwünschten Sinne einzubringen. Anerkannte Lebensleistungen und Seriosität in einer **unabhängigen Rolle** werden von Projektpartnern anerkannt und geschätzt. Neutralität bei der Behandlung von Fragen ist gewährleistet. Experten können aus dem Kreis der Forscher, Anwender oder auch der Industrie gewonnen werden.

Wirtschaftliche Interessen stehen nicht im Vordergrund. Dennoch ist eine **angemessene Förderung** der Mitarbeit erforderlich, die über die Erstattung spezifischer Einzelkosten hinausreicht, wie sie im Rahmen der assoziierten Partnerschaft vorgesehen ist. Der Begriff des Assoziierten Partners ist definiert und belegt; vorgeschlagen wird daher die zusätzliche Einführung des Senior-Experten als optionaler Projektpartner.

2.4.3 Handlungsempfehlungen

Der Begriff der Assoziierten Partnerschaft im Bereich SiFo muss definiert werden.

Die Einführung eines **Senior-Experten** als unabhängiger Partner im Projekt wird empfohlen.

Senior-Experten sollten, wie die assoziierten Partner auch, **nicht** der fallweise begrenzten Anzahl der Projektpartner zugerechnet werden.

Die Leistungen eines Senior-Experten müssen in **angemessener** Weise entgolten werden. Die Anlehnung der Stundensätze an solche von Projektleitern im Forschungsbereich erscheint bei nachgewiesener und anerkannter Qualifikation als angemessen.

2.4.4 Literatur

[DB]: DB Management Support, Ausführungen zum Einsatz von Senior-Experten, https://www.db-managementsupport.com/projektbezogene-unterstuetzung/vorteile-des-einsatzes-unserer-senior-experten.aspx, last visited 13.09.2022.

[ManMag 2000]: Die Vor- und Nachteile von Senior-Consulting-Firmen, https://www.manager-magazin.de/unternehmen/die-vor-und-nachteile-von-senior-consulting-firmen-a-8bade249-0002-0001-0000-000015855295, last visited 13.09.2022.

2.5 Internationale Zusammenarbeit mit der Ukraine

2.5.1 Kurzfassung

Internationale Zusammenarbeit in einschlägigen Forschungsprojekten, insbesondere mit Einrichtungen und Forschern der Ukraine, kann vorteilhaft zur Stärkung von Resilienz im Bereich Cyber-Sicherheit dienen. Eine Förderung auch solcher Projektkonstellationen wäre wünschenswert und kann die Erfahrungsbasis nachhaltig ausweiten. Politisch kann eine solche Initiative positiv wirken.

2.5.2 Themenfeld

Russlands Angriff auf die Ukraine hat die europäische und internationale Sicherheitsordnung verändert. Kanzler Scholz spricht von einer Zeitenwende mit daraus folgenden Verpflichtungen zum Überdenken von Positionen und Auswirkungen auch auf die Sicherheitsforschung und deren Anerkennung in der Gesellschaft.

Folgender Aspekt liefert zusätzliche Hinweise. Zitat, ins Deutsche übersetzt: *„Cyberkriegsführung ist ein Bestandteil der Konfrontation zwischen Russland und der Ukraine seit dem Zusammenbruch der Sowjetunion im Jahr 1991. Während die ersten Angriffe auf Informationssysteme privater Unternehmen und staatlicher Einrichtungen der Ukraine während der Massenproteste im Jahr 2013 verzeichnet wurden, gab es die russische Cyberwaffe Uroburos bereits seit 2005. Die russische Cyberkriegsführung setzte sich mit dem Hack des ukrainischen Stromnetzes zu Weihnachten 2015 und erneut 2016, der Lähmung des ukrainischen Finanzministeriums im Dezember 2016, einem Massenhackerangriff auf die Lieferkette im Juni 2017 und Angriffen auf ukrainische Regierungswebsites im Januar 2022 fort.“* [Wiki RuUk].

Seit vielen Jahren müssen sich die einschlägigen Sicherheitskräfte in der Ukraine mit Cyber Angriffen und der Entwicklung geeigneter Gegenmaßnahmen auseinandersetzen. Es gibt eine Erfahrungsbasis mit wertvollen Erkenntnissen zu Methoden und Angriffsstrategien.

Gemeinsame IT-Projekte waren auch in der Zeit vor dem 24.02.2022 Bestandteil der wirtschaftlichen Zusammenarbeit von Unternehmen und Forschungseinrichtungen und basierten auf erprobten und bewährten Modellen und Prozessen der Zusammenarbeit und Kommunikation. Insofern bestehen keine besonderen Hemmnisse.

2.5.3 Handlungsempfehlungen

Die Einbeziehung auch internationaler Projekte in die Fördermodelle sollte vorgesehen werden. Insbesondere die Ukraine erscheint als interessanter und wertvoller Partner.

2.5.4 Literatur

[Wiki RuUk]: Russian–Ukrainian cyberwarfare, https://en.wikipedia.org/wiki/Russian%E2%80%93Ukrainian_cyberwarfare, last visited 12.09.2022.

[CSIS, 2022]: James A. Lewis, Center for Strategic & International Studies, Cyber War and Ukraine, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?S.iEKeom79InugnYWlcZL4r3Ljuq.ash, last visited 12.09.2022.

3 Projektvorschläge

3.1 Vorbemerkungen

Die Bereiche innere und öffentliche Sicherheit umfassen eine breite Palette relevanter Themen. Menschenrechte, nationale Verfassungen und Gesetze definieren typischerweise die spezifischen Aufgaben und Zuständigkeiten hoheitlicher Organisationen und Einrichtungen.

Die Ausführungen zu den Rahmenbedingungen werden im Folgenden durch verschiedene Projektvorschläge ergänzt. Diese sollen einen Eindruck vom erwarteten Bedarf vermitteln und damit Hinweise auf Strukturen zukünftig erhoffter Förderprogramme liefern.

Das gesamte Marktvolumen betrug im Jahr 2014 ca. 238 Mrd. US-Dollar. Das Volumen teilt sich in ca. 28,4% für Antiterrormaßnahmen, 19,5% für IT- und Cyber-Sicherheit, 12% für kritische Infrastrukturen, 8,8% für die Grenzsicherung, 8,6% für die Sicherheit in der Luftfahrt, 7,0% für maritime Aufgaben und 3,5% für den öffentlichen Verkehr (Vision Gain: Homeland Security Market Forecast 2014-2024).

Der Sicherheitsmarkt ist ein wachsender Markt. Innovation ist der Türöffner für Start-Ups und engagierte Unternehmer. Kleine und mittlere Unternehmen (KMU) sind als Zulieferer im Markt akzeptiert und willkommen. Die Sorge um Sicherheit für die Gesellschaft und die Bevölkerung erfordert die Beschäftigung mit den folgenden Themenkreisen: Kriminalität im Allgemeinen Organisierte Kriminalität asymmetrische Bedrohungen Terrorismus Angriffe auf kritische Infrastrukturen Schmuggel und illegaler Waffenhandel Schleusung von Flüchtlingen illegale Prostitution Piraterie illegale Einwanderung Grenzsicherheit.

Die Ermutigung von Unternehmen, den Markt zu bedienen, ist somit auch wirtschaftlich begründbar und wertvoll.

3.2 Monitoring sozialer Medien

3.2.1 Autor

Prof. Dr. Ulrich Schade
Forschungsgruppenleiter FHG FKIE ITF
Ulrich.schade@fkie.fraunhofer.de

3.2.2 Kurzfassung

Soziale Medien werden für Kampagnen genutzt, mit denen die demokratische Rechtsordnung geschwächt werden soll. Solche Kampagnen sollten erkannt und analysiert werden.

3.2.3 Themenfeld

In öffentlichen Sozialen Medien werden beliebige Inhalte der Öffentlichkeit zugänglich gemacht. Dazu gehören Beeinflussungskampagnen mit dem Ziel, die demokratische Rechtsordnung zu schwächen. Solche Kampagnen beeinträchtigen die innere Sicherheit insbesondere dann, wenn Einzelmeinungen genutzt werden, um durch den Einsatz von Bots und durch Algorithmen, die Echokammern schaffen, Verschwörungstheorien bedient werden oder der Anschein einer Mehrheitsmeinung erweckt wird. Beispielsweise wurden im Mai 2022 Tweets von Sahra Wagenknecht und von Alice Weidel über dasselbe Netz als Re-Tweets verbreitet, um gegen Waffenlieferungen für die Ukraine Stimmung zu machen. Erst die Kenntnis von solchen Kampagnen ermöglicht eine Aufklärung gegen sie, was wiederum die Resilienz der Gesellschaft stärkt.

3.2.4 Forschungsbedarf

In den Beiträgen in den Sozialen Medien, die auf eine Beeinflussung abzielen, werden kritische Textpassagen, also diejenigen über die man automatisiert die kritischen Beiträge identifizieren könnte, zunehmend durch sogenannte Adversariale verschleiert. Ein Beispiel, die Selbstbeschreibung eines Twitteraccounts, lautet etwa "Řυsslдиð íšť иicħт ðęя Ғêiиð, ðəя циs υeяиíčħтeй шíłł. Ðíé Цкяaiиə υěятəiðígт иiçħт υиšêяe Шəятə. Циsęяə éìgêиə Řəgìěяциg υēяяaäт циš ғüŕ aмəяiқ. Ìñťęяęśśəи.“ Menschen können solche Adversariale lesen und verstehen, aber automatische Filter greifen hier nicht, sodass auf diese Weise "Hate Speech", Propaganda etc. nicht automatisiert erkannt, wohl aber von Menschen als solche verstanden werden. Die Wirksamkeit der Adversariale und die Möglichkeiten ihrer Identifikation sollten erforscht werden.

3.2.5 Anwendungspotenzial

Systeme, mit denen Beeinflussungskampagnen in den öffentlichen Sozialen Medien erkannt werden können, erleichtern beispielsweise die Arbeit von Rechercheteams, die auf Faktenchecks spezialisiert sind. Sie unterstützen damit die Aufklärung gegen derartige Beeinflussungen.

3.2.6 Literatur

Butter, M. (2021). Verschwörungstheorien: Eine Einführung. *APuZ*, 35-36/2021, 4-11.

Xu, H., Ma, Y., Liu, H.-C., Deb, D., Liu, H., Tang, J.-L. & Jain, A.K. (2020) Adversarial attacks and defenses in images, graphs and texts: A review. *International Journal of Automation and Computing*, ***17***, 151-178.

Zowislo-Grünewald, N. & Wörmer, N. (2021) (Hrsg.). Kommunikation, Resilienz und Sicherheit. Berlin: KAS.

3.3 Lieferkettensorgfaltspflichtengesetz (LKSG)

3.3.1 Autor

Anton Kramm
Analytical Semantics AG
a.kramm@analyticalsemantics.com

3.3.2 Kurzfassung

In den Unternehmen herrscht enorme Unsicherheit wie die Anforderungen zu Transparenz und Compliance in den Lieferketten erhoben und beurteilt werden können. Die hierzu ab 2023 verpflichteten Konzerne reichen die Anforderungen an die Bewertung der Lieferketten an ihre Zulieferer weiter. Das LKSG fordert neben einem transparenten Aufzeigen der Lieferkette entsprechende Erklärungen zu Menschenrechten, Nachhaltigkeit und Compliance entlang der gesamten Lieferkette für alle Zukaufprodukte in den Unternehmen. Globalisierung führt hier zu weltweiten Recherchen und Beurteilungen, ja sogar zur Ermittlung der Einzelbestandteile von Zukaufprodukten und Rohstoffen im Produktentstehungsprozess.

3.3.3 Themenfeld

Die Vorgaben des LKSG bedingen den Einsatz neuer innovativer Technologien wie intelligente Webcrawler und Suchmaschinen, ein etabliertes Risikomanagement für die Bewertung der Lieferanten und am Ende einen volldigitalisierten Bestell- und Beschaffungsprozess. Die heute bei den Lieferanten etablierten ERP und CRM Systeme richten jedoch ihre Funktionen auf die internen Prozesse der Unternehmen aus. Risikomanagement und Domainübergreifende Prozessdigitalisierung liegen in den Plattformen nicht vor. Der für das LKSG notwendige Einsatz von KI basierenden Textanalysesystemen, mehrsprachig und kontextabhängig, die Verbindung von strukturierten und unstrukturierten Daten in einem Frontend für die Bewertung von Lieferketten besteht nicht. Prozesse für die Risikobewertung der Ergebnisse, Einhaltung der Meldepflichten und entsprechender Prüfungen der Lieferanten wird systemseitig nicht unterstützt. Schnittstellen zu den Kernprozessen in den ERP und CRM Systemen, die je nach Analyseergebnis bereits gestartete Vorgänge stoppen oder anpassen sind nicht vorhanden.

3.3.4 Forschungsbedarf

Für eine Umsetzung der durch das LKSG geforderten Bewertungen und Maßnahmen ist es notwendig, alle Unternehmenssysteme in einer einheitlichen Schicht vorzuhalten und dennoch den Zugriff auf diese Schicht nur mit anonymisierten Informationen anzuzeigen. Derzeitige Suchmaschinen und Webcrawler erlauben mit hohem Aufwand die Erstellung dieser Informationsschicht und zum Teil auch den Aufbau von Verbindungsgrafen. Die direkte Interaktion dieser Informationsschicht mit den etablierten Prozessen und damit einhergehender Risikobeurteilung und der sich am Ende ergebenden Reaktion für die Beschaffungs- und Bestellprozesse oder Lieferantenbewertung sind derzeit keine integrierten Technologien am Markt verfügbar. Ein weiteres offenes Thema stellen die fachlichen Vorgaben in Bezug auf die Attribuierung und Merkmale für die Risikobewertungen der gelieferten Informationen dar. Wann, bei welchen Scores aus welchen Quellen ist stufenweise zu agieren, welche Maßnahmen können ergriffen werden, wie sind die Prozesse in und Systeme in welchen Zeiträumen anzupassen.

3.3.5 Optionales Anwendungspotenzial

Jedes Unternehmen hat sich dem LKSG zu stellen und diese umzusetzen. Derzeit werden auf Grund fehlender Technologien alle beschriebenen Themen manuell durch unterschiedliche Prozesse versucht zu lösen. Dennoch entsteht keine Rechtssicherheit, Daten bleiben erhalten, sind zwangsläufig unvollständig und in einem babylonischen Sprachenmix vorhanden. Der Verantwortliche ist derzeit nicht in der Lage wirklich rechtskonform zu agieren. Der Aufwand für diese mangelhaften Ergebnisse für die Recherche und bei der Durchführung liegt im mehrtägigen Bereich. Eine entsprechende technologische Lösung würde neben einer Steigerung der Qualität (> 95%) zu einer Reduktion der Aufwände um bis zu 90% führen. Die Einhaltung der rechtlichen Vorgaben erzwingt den Einsatz der Technologie und

schafft für das Unternehmen darüber hinaus volle Transparenz über die vorhandenen Daten. Grundsätzlich ist jedes Unternehmen verpflichtet eine entsprechende Plattform einzuführen. Neben der Erfüllung der LKSG Vorgaben sind auch weitere Themen wie Risikomanagement, Lieferantenbewertung, Prozessdigitalisierung damit abzubilden und zu bedienen.

3.3.6 Handlungsempfehlungen

Für die Umsetzung erscheint die nachfolgende Paketierung geeignet, da die einzelnen Ergebnisse für sich bereits Mehrwerte und Erkenntnisse in sich darstellen: - Erarbeitung des notwendigen Contents in Bezug auf die relevanten Vorgaben und Bewertungsmatrizen sowie Korrelation der internen Lieferantendaten in einer Risikomatrix - Erarbeitung des entsprechenden Regelwerks in Kombination zu Rechercheergebnissen - Produktvergleich und Integrationsmöglichkeiten der unterschiedlichen Basissystem zu einer neuen übergreifenden und bedienbaren Plattform, ausgerichtet auf die fachlich verantwortlichen Anwendergruppen - Realisierung einer Plattform als Datenhaltungs- und Erhebungsschichtindung zwischen Such-, Webcrawlern mit Schnittstellen zu den wichtigsten Datenhaltungssystemen (ERP, CRM, Office Pakten, eMail Systeme, ausgewählte social media channels (instagram, linkedin) und Digitalisierung der Meldeprozesse sowie der Prozessinteraktion mit den Lagacy Systemen - Pilotimplementierung realer Interessent

3.3.7 Literatur

Lieferkettensorgfaltspflichtengesetz, Risikomanagement ISO 37010

3.4 Aspekte zum Datenschutz – Löschen und Qualitätsmanagement

3.4.1 Autor

Anton Kramm
Analytical Semantics AG
a.kramm@analyticalsemantics.com
+01706344618
Danziger Straße 64
85276 Pfaffenhofen a.d. Ilm

3.4.2 Kurzfassung

In den Unternehmen und bei den Bürgern herrscht enorme Unsicherheit in Bezug auf die Vollständigkeit von Datenlöschungen entweder auf Grund eines Löschersuchens eines Betroffenen oder der Löschung auf Grund von Aufbewahrungsfristen. Gerade die unterschiedliche Art der Datenspeicherung (Datenbanken, Systeme, Excel, word, social media Kanäle) führt zu dieser Unsicherheit und zur mangelnden Transparenz bei der Einhaltung der gesetzlichen Vorgaben.

3.4.3 Themenfeld

Die durch die DSGVO etablierten Vorgaben zur Löschung und Auskunft der Betroffenen in Bezug auf ihre persönlichen Daten stellt die Unternehmen vor enorme Herausforderungen diesem berechtigten Interesse nachzukommen. Die verteilte Datenhaltung in Systemen wie ERP, CRM und social media channels, aber auch in Tabellenprogrammen, Dokumenten, eMail und Anhänge oder Datenbanken führt dazu, dass derzeit die Recherche bei einem Löschersuchen nicht nachweislich durchgeführt werden kann. Die Verbindungen der Daten über Systeme und Informationen hinweg ist mit derzeitigen konventionellen Mitteln nicht realisierbar, gerade unter Einbeziehung personenbeziehbarer Daten. Der Datenschutzbeauftragte bzw. Datenschutzverantwortliche muss jedoch sicherstellen, dass unabhängig vom Grund der Löschung alle diese Daten gelöscht werden können. Hierzu fehlt es derzeit neben der Fähigkeit alle diese Daten zu finden, an der Verknüpfung personenbezogener zu personenbeziehbaren Daten über System- und Informationsarten hinweg. Es ist nicht möglich einen übergreifenden logischen Verbindungsbaum aufzubauen und dann dediziert die notwendigen Löschungen

3.4.4 Forschungsbedarf

Für eine Umsetzung der durch die DSGVO geforderten Löschung bzw. Löschersuchen ist es notwendig alle Unternehmenssysteme in einer einheitlichen Schicht datenschutzkonform vorzuhalten und dennoch den Zugriff auf diese Schicht nur mit anonymisierten Informationen anzuzeigen. Derzeitige Suchmaschinen erlauben mit hohem Aufwand die Erstellung dieser Informationsschicht und zum Teil auch den Aufbau von Verbindungsgrafen, aber spätestens mit der Anonymisierung und der sich am Ende ergebenden Durchführung der Löschung sind derzeit keine Technologien am Markt verfügbar. Auch die Funktionen zum regelbasierenden Aufbau der zweckbezogenen Löschfristen zu den Informationsquellen und dann deren Integration und Anbindung an die Auswerteschichten existieren nicht. Ein weiteres offenes Thema stellen die fachlichen Vorgaben in Bezug auf die Attribuierung personenbezogen-personenbeziehbare Daten zur Zweckorientierung und damit Löschfrist dar. - Aufbau der Korrelationen zwischen unterschiedlichen Löschfristen auf Grund der Zweckbindungen zu den verschieden Informationssystemen bei abweichender Zweckbindung - Ermittlung der Beziehungsattribute von personenbeziehbaren zu personenbezogenen Daten. - Statement zum Einsatz dieser Technologie (Profiling) in Bezug auf die DSGVO Vorgaben. - Technische Lösung / Schwärzung von z.b. eMail Anhängen und eMails - Automatische Löschung von Zeilen aus Tabellenkalkulationsprogrammen

3.4.5 Anwendungspotenzial

Jedes Unternehmen hat sich der DSGVO zu stellen und diese umzusetzen. Derzeit werden auf Grund fehlender Technologien alle beschriebenen Themen manuell durch unterschiedliche Prozesse versucht zu lösen. Dennoch entsteht keine Rechtssicherheit, Daten bleiben

erhalten. Der Datenschutzverantwortliche ist derzeit nicht in der Lage wirklich rechtskonform zu agieren. Der Aufwand für diese mangelhaften Ergebnisse für die Recherche und bei der Durchführung der Löschung liegt dennoch im mehrtägigen Bereich. Eine entsprechende technologische Lösung würde neben einer Steigerung der Qualität (> 95%) zu einer Reduktion der Aufwände um bis zu 90% führen. Die Einhaltung der rechtlichen Vorgaben erzwingt den Einsatz der Technologie und schafft für das Unternehmen darüber hinaus volle Transparenz über die vorhandenen Daten. Grundsätzlich wäre jedes Unternehmen verpflichtet eine entsprechende Plattform einzuführen, wenn dies wirtschaftlich vertretbar ist. Neben der Erfüllung der DSGVO Vorgaben sind auch alle weiteren Themen wie Aufbewahrung, Löschung usw. aus anderen Rechtsgebieten wie Steuer (AO), HGB, BGB damit abzubilden und zu bedienen.

3.4.6 Handlungsempfehlungen

Für die Umsetzung erscheint die nachfolgende Paketierung geeignet, da die einzelnen Ergebnisse für sich bereits Mehrwerte und Erkenntnisse in sich darstellen: - Erarbeitung des notwendigen Contents in Bezug auf die Korrelation der Daten - Erarbeitung des entsprechenden Regelwerks in Kombination zu Zweckbindungen - Abstimmung und gutachterliche Beschreibung der Einsatzmöglichkeiten - Produktvergleich und Integrationsmöglichkeiten der unterschiedlichen Basissystem - Realisierung einer Plattform zur Verbindung zwischen Such-, Profiling und Rulesengines mit Schnittstellen zu den wichtigsten Datenhaltungssystemen (ERP, CRM, Office Pakten, eMail Systeme, ausgewählte social media channels (instagram, linkedin) - Pilotimplementierung realer Interessent.

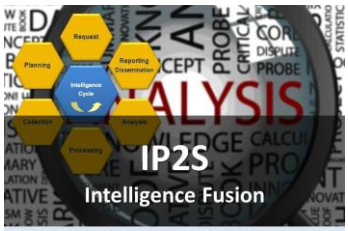
3.4.7 Literatur

Datenschutzgrundverordnung, Bundesdatenschutzgesetz

3.5 DITS – diverse Projektvorschläge

DITS verfolgt insbesondere Projekte und Initiativen.

3.5.1 IT Assistenzsysteme



Die konsequente Erfassung, Verarbeitung und Verdichtung von Informationen ist beste Voraussetzung für gute Entscheidungen.

Lesen Sie weiter ...

https://www.dits.center/indexspot31_g.html

Die Verifikation von Angaben zum Beispiel zur Person und der Herkunft ist ein Themenfeld, das in verschiedenen Bereichen eine wichtige Rolle spielt.

Lesen Sie weiter ...

https://www.dits.center/indexspot32_g.html

Globale Wertschöpfungsketten werden von illegalen Aktivitäten bedroht. Betrug, Diebstahl, Schmuggel, Markenpiraterie, Wirtschaftsspionage und Compliance sind Herausforderungen.
Lesen Sie weiter ...

https://www.dits.center/indexspot34_g.html

3.5.2 Sensoren

Die Lokalisierung und Verfolgung von Funkemittern ist eine herausfordernde Aufgabe für Sicherheits- und Regulierungsbehörden.

Lesen Sie weiter ...

https://www.dits.center/indexspot41_g.html

Drohnen sind interessante Plattformen für Sensoren zur Identifikation und Klassifikation von unterschiedlichen Funkemittern.

Lesen Sie weiter ...

https://www.dits.center/indexspot42_g.html

Die Nutzung der Signalszenarien aus Mobilfunknetzen erlaubt neue und innovative Konzepte zur Ortung von Objekten.

Lesen Sie weiter ...

https://www.dits.center/indexspot53_g.html

3.5.3 Prävention

Ladendiebstahl ist kein Kavaliersdelikt und kann mit intelligenter Technik effektiv verhindert werden.

Lesen Sie weiter ...

https://www.dits.center/indexspota1_g.html

Die Erkennung bedrohlicher Szenarien ohne Belästigung der Kunden und Besucher ist eine anspruchsvolle Aufgabe für intelligente Technik.

Lesen Sie weiter ...

https://www.dits.center/indexspota2_g.html

Die Versorgung mit Wasser, Nahrung, Energie und diversen Dienstleistungen muss trotz vielfältiger Bedrohungen gesichert werden.

Lesen Sie weiter ...

https://www.dits.center/indexspota3_g.html

Frachtdiebstahl verursacht jährlich Schäden in Milliardenhöhe. Technik hilft, Ladung und Mitarbeiter zu schützen.

Lesen Sie weiter ...

Drohnen sind weit verbreitet. Das Bedrohungspotenzial für die Bevölkerung und kritische Infrastrukturen ist extrem hoch.

Lesen Sie weiter ...

Industrie 4.0 fördert die Vernetzung in komplexe Systemen zur Prozesssteuerung. Sicherheit muss auch von KMUs gewährleistet werden.

Lesen Sie weiter ...

https://www.dits.center/indexspota4_g.html https://www.dits.center/indexspota5_g.html https://www.dits.center/indexspot33_g.html

3.5.4 Studien und Initiativen

Das Bundesministerium für Bildung und Forschung bietet diverse differenzierte Fördermöglichkeiten von Forschungsprojekten für Anwender, Forscher und die Industrie – insbesondere auch für KMUs.
Lesen Sie weiter ...

https://www.dits.center/indexspot81_g.html

Sicherheit und Freiheit beschäftigen die Gesellschaft und dürfen bei der Entwicklung von Technik nicht unberücksichtigt bleiben.

Lesen Sie weiter ...

https://www.dits.center/indexspot82_g.html

Sicherheitsforschung könnte ein neuer Schwerpunkt mit interessanter Marktperspektive für die Metropolregion Nürnberg werden.

Lesen Sie weiter ...

https://www.dits.center/indexspot83_g.html

3.5.5 Professionelles Projektmanagement

Lösungsorientierte Forschung entfaltet sich nur mit der Einbeziehung des Anwenders und der Industrie. DITS unterstützt in vielfältiger Weise.

Lesen Sie weiter ...

https://www.dits.center/indexspot84_g.html

DITS.center e.V. wurde 2016 als gemeinnütziger Verein von einem Team hochdiversifizierter, exzellenter Experten nach deutschem Recht gegründet. Die Gründungsmitglieder folgten ihren Idealen und unterstützen den Verein mit ihren einschlägigen Erfahrungen aus jahrzehntelanger erfolgreicher beruflicher Tätigkeit in Praxis und Führung.

DITS verfolgt das nicht-kommerzielle Ziel, angewandte Forschung in Projekten der zivilen und öffentlichen Sicherheit, einschließlich der Kriminalitätsprävention, zu fördern. Der Verein unterstützt nationale und internationale Zusammenarbeit, Technologietransfer, den Informationsaustausch sowie den Dialog zwischen verschiedenen Institutionen und Organisationen.

DITS konzentriert sich auf Forschungs- und Entwicklungsprojekte, die einen Beitrag zur Sicherheit und dem Schutz von Einrichtungen und Strukturen leisten. Geeignete Dienstleistungen werden erbracht, um den Informationsaustausch, die Ideenfindung und die Zusammenarbeit zwischen Wissenschaft, Anwendern und Industrie zu fördern.

DITS ist bestrebt, alle Arten von Technologien zu unterstützen und zu fördern, die einen vielversprechenden Beitrag zu sicherheitstechnischen Innovationen leisten.

DITS arbeitet kreativ an der Förderung und Durchführung anwendungsorientierter Forschung auf dem Gebiet der Signalerfassung, -analyse und Informationsverarbeitung. Anerkannte methodische Standards werden genutzt, um grundlegende Fragen in ihren Ursachen und Zusammenhängen zu untersuchen und Forschungsergebnisse in Anwendungen zu überführen.

DITS.center e.V.

www.DITS.center