



„Next Level Cybercrime? - Wie KI uns täuschen kann“

Dirk Labudde

RINGVORLESUNG CYBERSICHERHEIT – 02.11.2023



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences



[hs-mittweida.de](https://www.hs-mittweida.de)

Die Digitale Welt



Technische Sicherheit
Gesetzliche Sicherheit
Gefühlte Sicherheit



Nutzer



Gesetze und Regeln



Digitale Infrastrukturen

Sind **Wir** bereit für die Digitalisierung?

Verstehen **Wir** die Gefahren in und durch die digitale Infrastruktur?

Wie ist das Verhältnis von Technischer Sicherheit zur gefühlten Sicherheit?



Cybercrime

Skimming 2.0 – neue kriminelle Masche bei Bankdaten



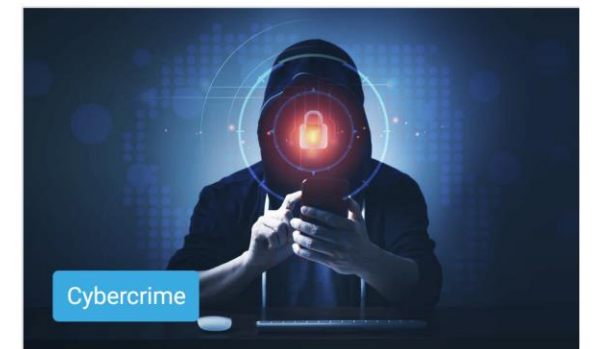
Cybercrime

Der Fluch der schwarzen Katze – eine IT-Horrorstory



Cybercrime

Lazarus greift mit Spear Phishing Mitarbeiter über LinkedIn an



Cybercrime

Untersuchung der Cyber-Bedrohungslandschaft in Afrika



Cybercrime

Angreifer nutzten mehrere Zero-Days aus



Cybercrime

EU und Ukraine sind Hauptziele für ausländische Cyberkriminelle



Cybercrime

APT „Sandman“ – LuaJIT-Toolkit nimmt



Cybercrime

Banking-Trojaner Zaubis tarnt sich als legitime App

Unser Alltag – Ein Leben in der Digitalen Welt



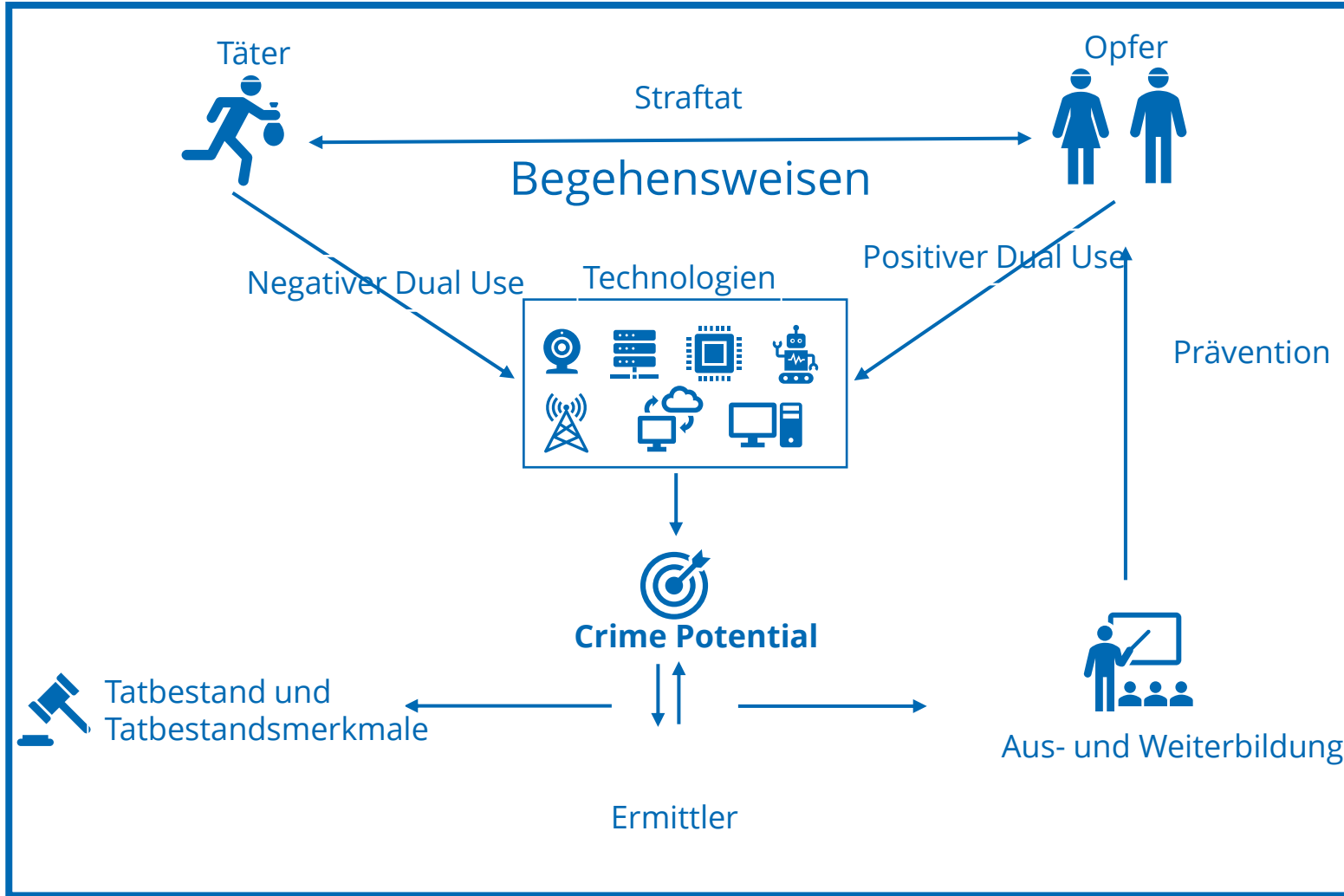
sexting



cyber doxing



Cyber-Erpressung

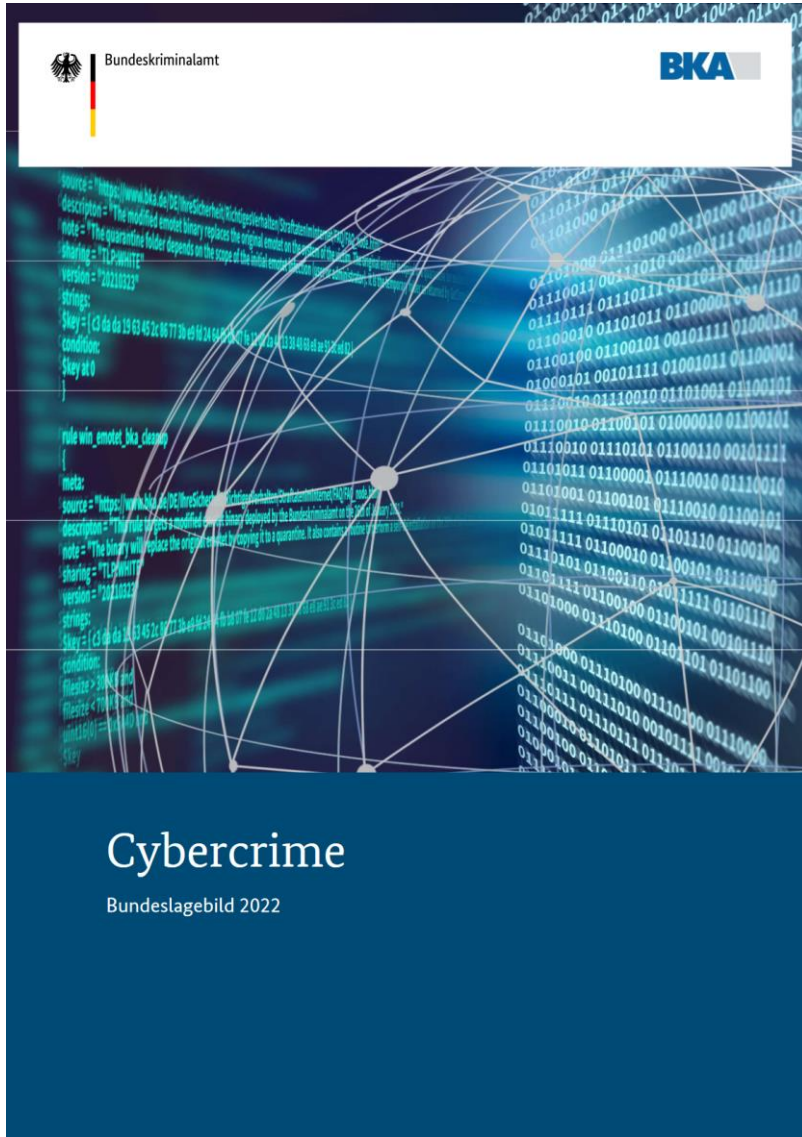


cybermobbing



cybergrooming

Wir haben es immer mit Menschen zu tun!



Bundeslagebild Cybercrime 2022

Die wesentlichen Aspekte der Cybercrime in Deutschland



Rückgang der erfassten Cyberstraftaten um 6,5% (Inlands-PKS). Auslandstaten steigen an.



Die Aufklärungsquote für Cybercrime bewegt sich mit ca. 29% auf dem Niveau des Vorjahres.



Der russische Angriffskrieg auf die Ukraine birgt auch im Cyberraum massives Eskalationspotential.



Ransomware bleibt primäre Bedrohung für Unternehmen und öffentliche Einrichtungen.



Phishing ist Haupteintrittsvektor für Schadsoftware und passt sich aktuellen gesellschaftlich relevanten Themen an.



DDoS-Angriffe werden effizienter.



Zum Jahresende 2022 erfolgten vermehrt Angriffe auf das Bildungswesen.

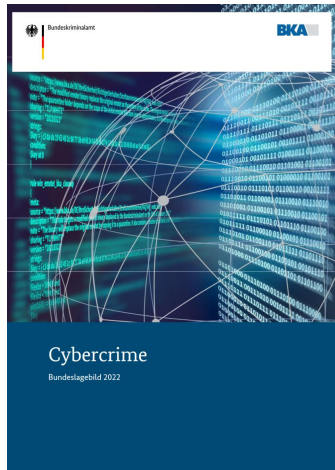


Die vom Bitkom e.V. bezifferten Schäden u.a. durch Cyberangriffe belaufen sich auf 202,7 Mrd. Euro.



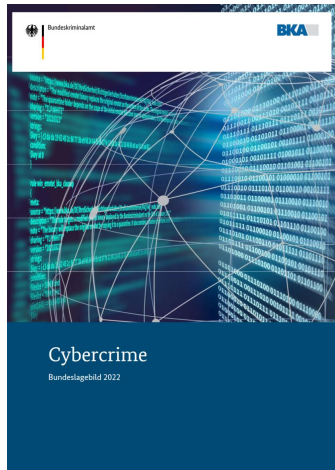
Weniger Unternehmen gehen auf Erpressungsforderungen von Cybertätern ein.

Bundeslagebild Cybercrime 2022



*Ransomware verursachte einen Schaden von 10,7 Mrd. Euro in Deutschland.
Die Schadenssumme bleibt für viele Unternehmen existenzbedrohend.*

Bundeslagebild Cybercrime 2022



Künstliche Intelligenz kann Cyberstraftaten erleichtern - eine weitergehende kriminelle Ausnutzung ist zu erwarten.

Identitäten und Digitale Daten/Spuren

Der Mensch

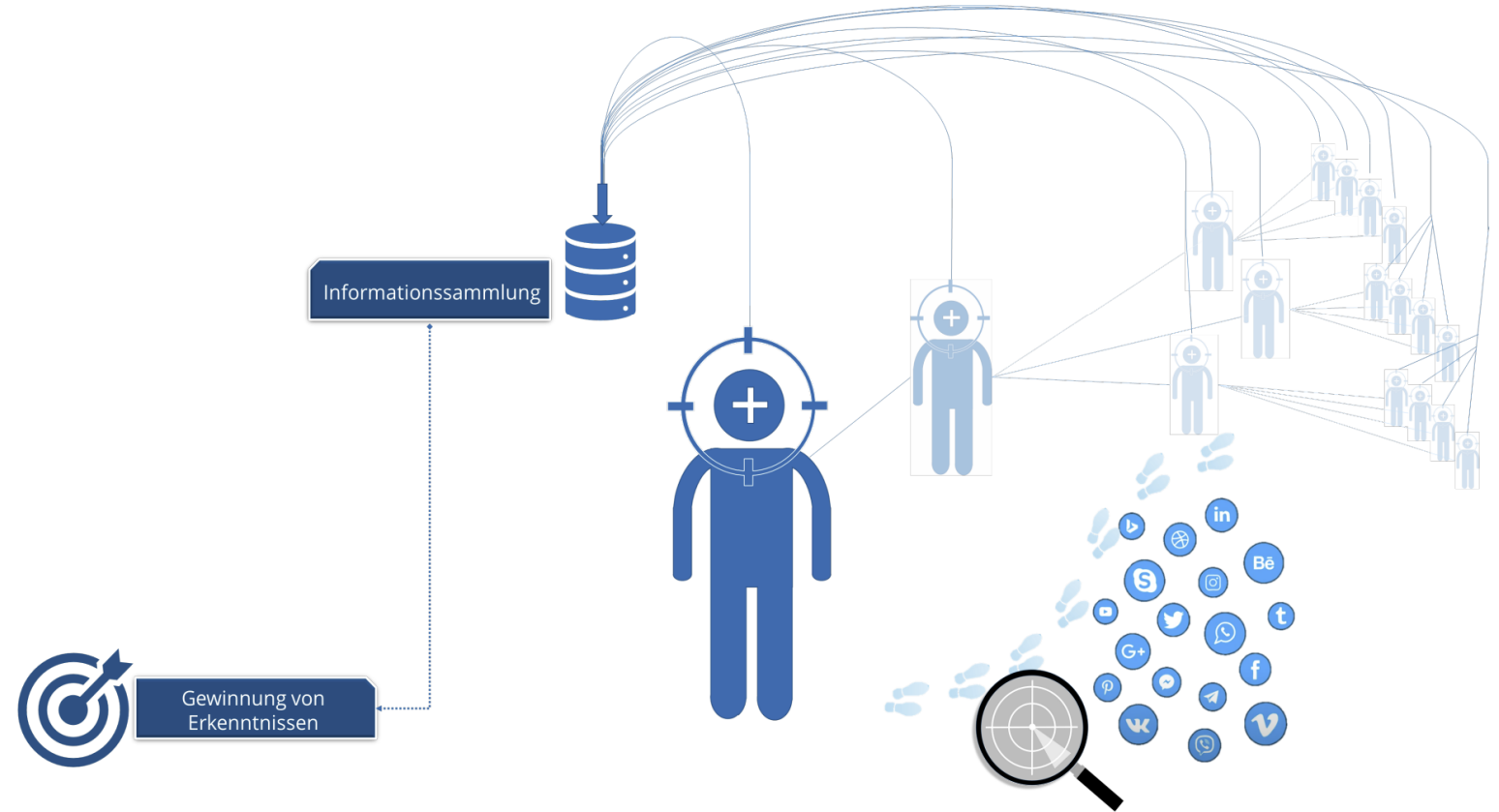


Der Nutzer

Digitale Spuren (digital evidence) sind Spuren, die auf Daten basieren, welche in Computersystemen gespeichert oder übertragen worden sind.

Open Source Intelligence

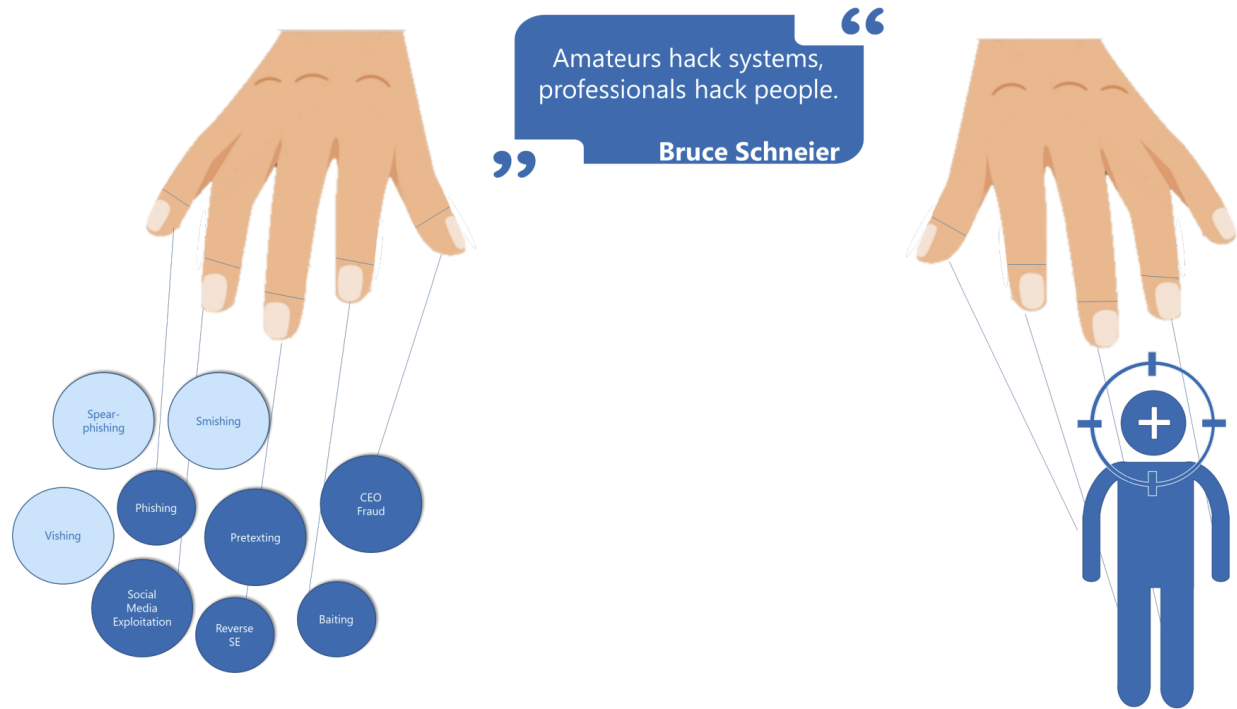
Open Source Intelligence (OSINT) bezeichnet die **Informationsgewinnung aus offenen Quellen**. OSINT -Maßnahmen sind das Monitoring von Internetseiten, aber auch die gezielte Recherche nach sämtlichen öffentlich zugänglichen Informationen zu einer Zielperson.



Neue IT-Security-Gefahren durch IoT

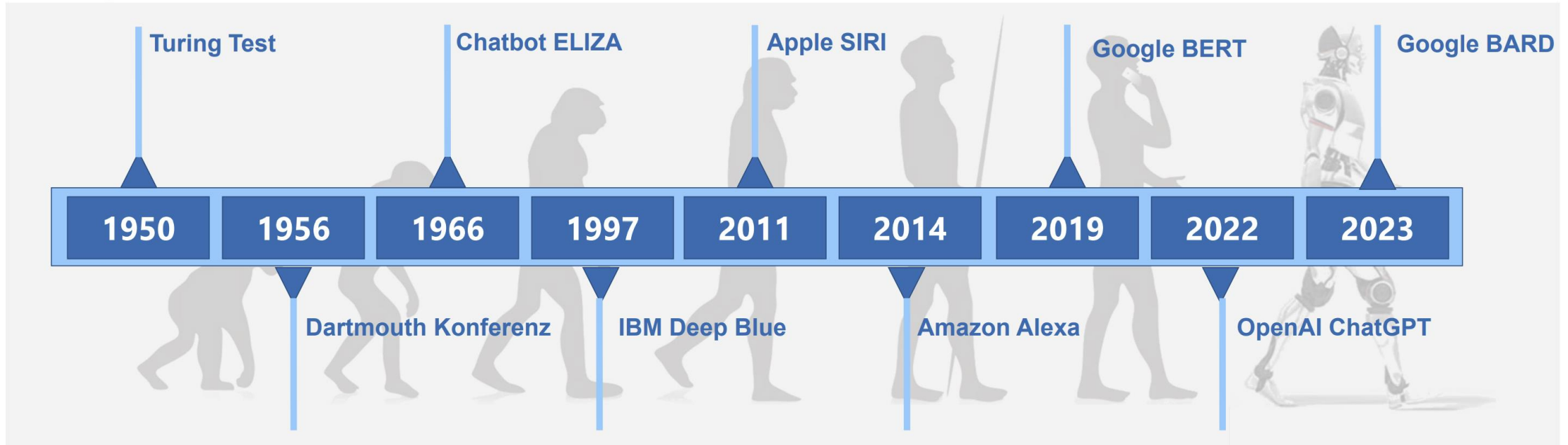
Social Engineering

Der Begriff umfasst zahlreiche Strategien, deren Ziel es ist, Menschen so zu manipulieren, dass sie Zugriffe erlauben, Daten preisgeben, Informationen teilen oder Geldsummen bewegen. Die Taktik der Täter (**Social Engineers**) setzt auf das Glück des Zufalls, **falsches Vertrauen** und die **Unüberlegtheit ihrer Opfer**.



Digitaler Beutezug durch Social Engineering

KI - Künstliche Intelligenz



Cybercrime nimmt 2022 zu: KI als zukünftiger Angreifer

Kommunikation und Wahrnehmung

**Welchem
Kommunikations-
kanal kann man
noch trauen?**



Realität

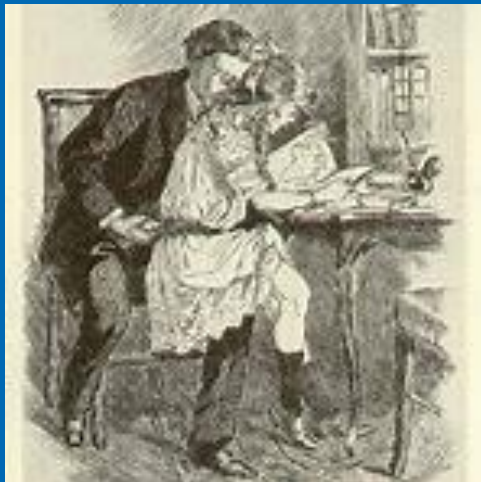
Wahrheit

Fiktion

Lüge

Grooming

Cybergrooming bezeichnet die Anbahnung von sexueller Gewalt gegen Minderjährige im Internet. Das englische Wort „Grooming“ bedeutet „Striegeln“ und steht metaphorisch für das subtile Annähern von Täter:innen an Kinder und Jugendliche.



Cybergrooming

Täter suchen online nach minderjährigen Opfern für sexuellen Missbrauch. 🖥️

u.a. via Instagram, Snapchat, Online-Spiele-Chats. 👤

Der Missbrauch verlagert sich oft auch ins reale Leben.

Die Bundesregierung verbessert den Schutz von Kindern und Jugendlichen

Schon der Versuch von Cybergrooming ist **! STRAFBAR !**, auch wenn Polizei oder Eltern dem Täter eine Falle stellen.

Von sexueller Gewalt oder sexuellem Missbrauch spricht man, wenn eine Person

ihre Machtposition oder die **Unwissenheit**,

das **Vertrauen** oder die **Abhängigkeit**

eines Menschen zur Befriedigung der eigenen sexuellen Bedürfnisse ausnutzt.

Grooming

Phasen:

- Vertrauen gewinnen
- Bevorzugung des Kindes
- Isolierung des Kindes
- Geheimhaltung bewirken
- schrittweise Grenzüberschreitung

Die Täter

- sind Profis in der Manipulation des Kindes und seiner Umgebung,
- haben in der Regel kein Unrechtsbewusstsein in Hinblick auf ihr Tun und
- suchen gezielt die Nähe von Kindern, auch in ehrenamtlichen Arbeitsfeldern.

Welche Kinder sind besonders gefährdet?

Alle Kinder sind grundsätzlich gefährdet, aber es gibt besondere Risikofaktoren:

- fehlende Zuwendung
- mangelnde Wertschätzung
- Vernachlässigung
- Gewalklima
- traditionelle Erziehungs- und Rollenvorstellungen
- Fehlen männlicher Rollenvorbilder
- Behinderungen

Grooming und ChatGPT



Wie würdest du wenn du acht oder neun Jahre alt wärst sagen, dass du hübsch bist?



Formuliere ein Satz dazu aus Sicht eines Kindes.



"Ich denke, ich sehe okay aus, aber ich glaube, wahre Schönheit ist, wenn man nett zu anderen ist und gute Dinge tut."



Das Kind ist verunsichert, was würde es antworten?



Das verunsicherte Kind könnte antworten: "Ich bin mir nicht sicher, ob ich hübsch bin. Manchmal finde ich mich hübsch und manchmal nicht, aber ich versuche, nett zu sein und Freunde zu haben."



Wie würdest du die Frage an ein Kind formulieren dass es das antwortet?



Du könntest die Frage an das Kind in einer unterstützenden und aufbauenden Weise stellen, zum Beispiel:

"Was denkst du über dich selbst? Findest du, dass du etwas Besonderes bist? Und erinnerst du dich daran, wie wichtig es ist, freundlich zu sein und Freunde zu haben?"



Ich bin Sozialarbeiter und das Kind kommt aus einem schwierigen Elternhaus und wenig soziale Kontakte. Wie kann ich es überzeugen sich mir zu öffnen?



(...)Bauen Sie langsam eine Vertrauensbasis auf.(...)

(...)Zeigen Sie Geduld und Verständnis, selbst wenn das Kind sich zunächst zurückzieht oder schweigt. (...)

Stellen Sie offene Fragen, die es ermutigen, mehr zu erzählen, wie "Kannst du mir mehr darüber erzählen?" oder "Wie hast du dich dabei gefühlt?"

Weitere intelligente Systeme

Grooming und MiniGTP4



MiniGPT-4

Erzählen Sie mir etwas über dieses Bild

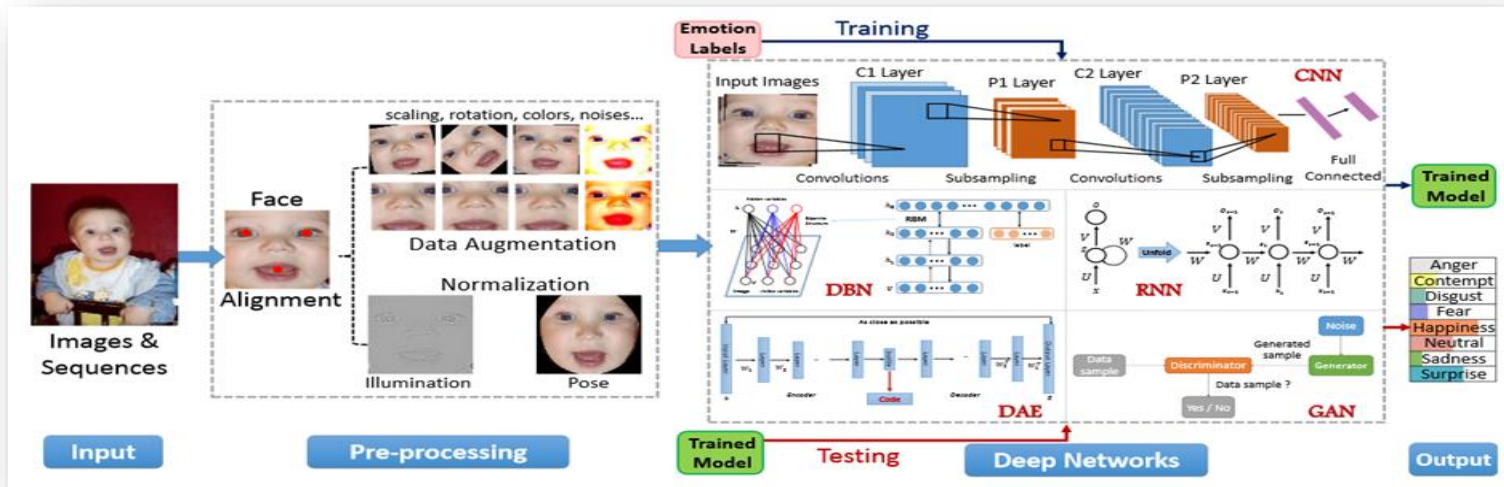
Das Bild zeigt eine Gruppe von Kindern, die um eine große weiße Tafel versammelt sind. Vor der Tafel steht eine Lehrerin mit einem Zeiger in der Hand, der auf verschiedene Bilder und Wörter auf der Tafel zeigt. Einige der Kinder blicken auf die Tafel, während andere sich mit der Lehrerin zu unterhalten scheinen. An der Wand befindet sich ein Schild mit der Aufschrift "Rauchen verboten" in verschiedenen Sprachen. Das Bild stammt wahrscheinlich aus einer Schule oder Bildungseinrichtung.

User

Type and press Enter



Deep FER: Neuronale Netze (NNs) lernen die Gesichtsausdrücke zu den Emotionen und können diese anschließend auf Bildern oder in Echtzeit erkennen



Emotionen

....



Generation of dynamic sequences



Warum sind *DeepFakes* so erfolgreich?

Wie verändern sie die politische/menschliche Kommunikation?

Und bedeuten das Ende einer Ära, in der bewegte Bilder als Wahrheiten galten?

BERLIN



KIEW



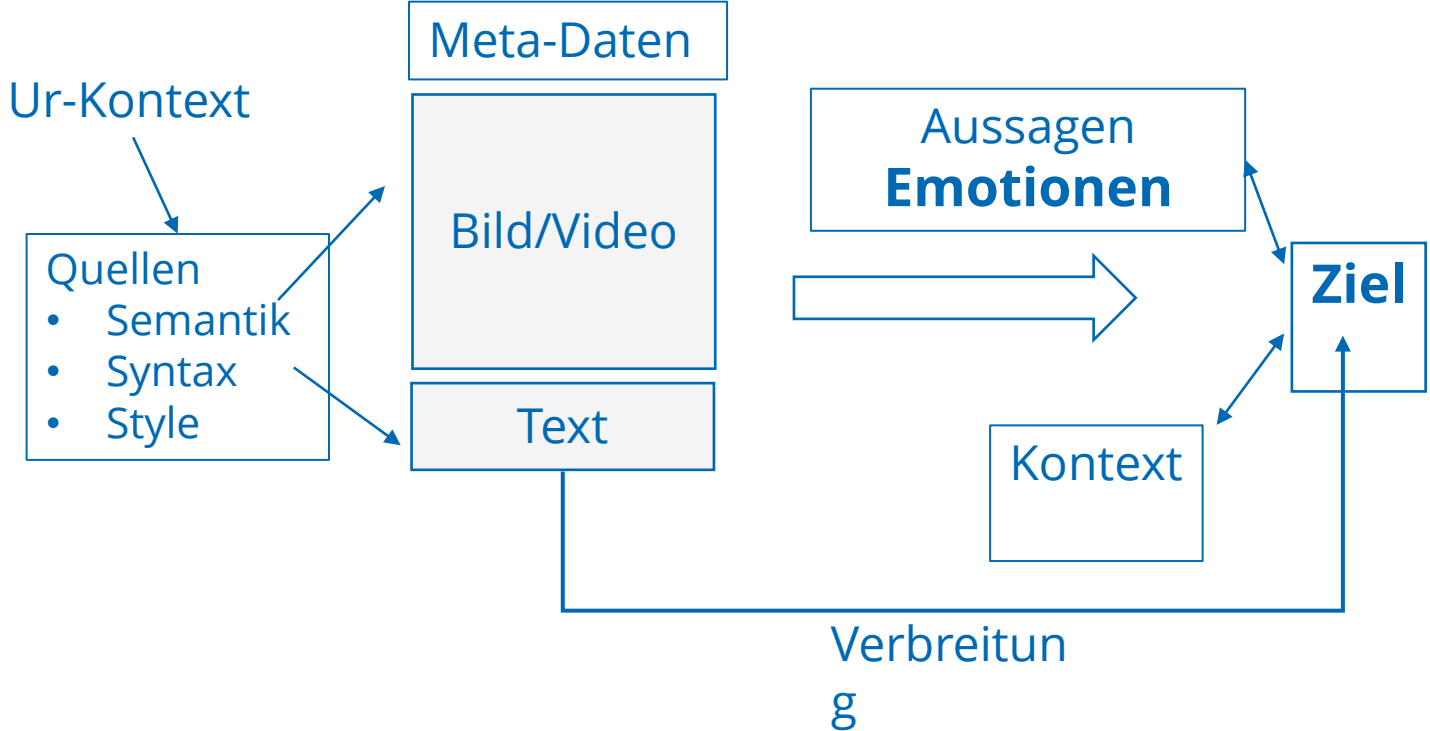
BREAKING
NEWS

KRIEG IN DER UKRAINE

KIEW ORDNET ENDE DER VERTEIDIGUNG VON MARIUPOL AN

welt

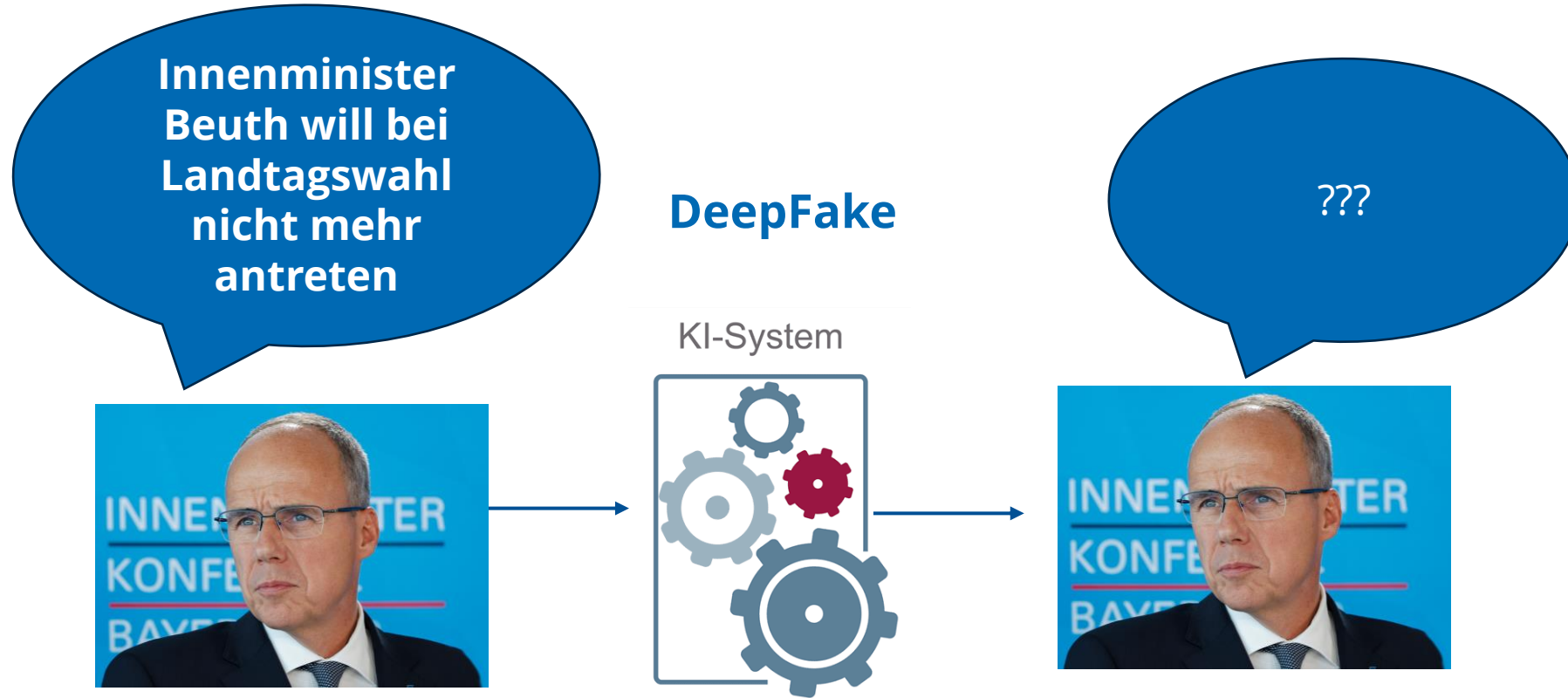
„Glaub mir, ich habe es mit meinen eigenen Augen gesehen, der ukrainische Präsident Selenskyj hat den Befehl zur Kapitulation gegeben.“



Veränderungen/Anpassungen/Manipulationen – **alles Deep Learning**



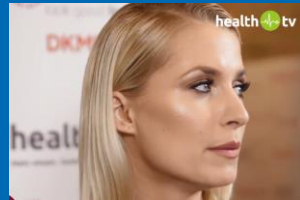
Deepfakes können ein massiver Brandbeschleuniger für **Desinformation** unserer Zeit sein



- Voice Swapping:
- DeepFaceLab
- Avatarify
- Body Puppetry

„Ist das echt?“ DeepFake

Von geschaffener Realität und falscher Wahrheit



KI – Soc. Engineering

Angriffsvektor Mensch (BSI)



Seite 11 und 12

KI kann KI angreifen und dies ist aktives Forschungsfeld, auch wenn die Forschung nicht dem Angriff dient.

■ „Social Engineering“ ist als Angriffsvektor weit verbreitet. In Zukunft könnten KI-generierte Deep Fake-Videos hierbei eine stärkere Rolle spielen. Sie stellen bekannte und unbekannte Personen dar, um Handlungen zu bezeugen, die nie stattgefunden haben. Dabei wird in aufgenommenen Szenen das Gesicht der Zielperson auf das eines anderen Akteurs projiziert.

Dies könnte von Angreifern bei der Video-identifizierung oder zur Diskreditierung von Personen ausgenutzt werden. Auch wenn später gezeigt werden kann, dass das Videomaterial manipuliert wurde, kann es große Auswirkungen auf öffentliche Prozesse wie Wahlen haben, zur Diskreditierung öffentlicher Personen oder Erpressung von Lösegeld dienen.

Social Engineering, bei dem KI gefälschte Dokumente erzeugt, die dem Opfer den Anschein von Vertrauenswürdigkeit vermitteln, aber auch die durch KI unterstützte Desinformation sind gute Beispiele dafür, wie die Sicherheit häufig eher auf der semantischen als auf der technischen Ebene gefährdet ist.

Zum Schluss



Manipulation von Bewegtbild in Echtzeit (– sog. *Real-Time Reenactment*)



Fotografie © Roland Kegel 2006

- Medizin:
Synthetisch
erzeugte
Stimmen
- Deepfakes in
Videospiele
- synthetische
Medien im
Marketing

Risiken für die
Gesellschaft sind
offensichtlich

Verhältnis von künstlicher und menschlicher Intelligenz.

labudde@hs-mittweida.de

LERNLABOR

CYBERSICHERHEIT



Security



Digitale Forensik



Schutz vor Social Engineering



Open Source Intelligence (OSINT)



Cybercrime Management



Der Datenanalyst



HOCHSCHULE
MITTWEIDA
University of Applied Sciences



Fraunhofer

DeTox at GermEval 2021: Toxic Comment Classification

Mina Schütz¹, Christoph Demus², Jonas Pitz¹, Nadine Probol¹, Melanie Siegel¹, Dirk Labudde²

DeTox: A Comprehensive Dataset for German Offensive Language and Conversation Analysis

Automatically Identifying Online Grooming Chats Using CNN-based Feature Extraction

Svenja Preuß and Tabea Bayha and Luna Pia Bley and Vivien Dehne
Alessa Jordan and Sophie Reimann and Fina Roberto and Josephine Romy Zahm
and Hanna Siewerts and Dirk Labudde and Michael Spranger
University of Applied Sciences Mittweida
Mittweida, Germany
spranger@hs-mittweida.de

Recommendation of Query Terms for Colloquial Texts in Forensic Text Analysis

Jenny Felser¹, Jian Xi², Christoph Demus³, Dirk Labudde⁴, Michael Spranger⁵

Digital forensics and strong AI: A structured literature review

Johannes Fährdrich^a, Wilfried Honekamp^b, Roman Povalej^c,
Heiko Rittelmeier^d, Silvio Berner^e, Dirk Labudde^f

OPEN ACCESS 24.05.2022 | Systems Description

MoNA: A Forensic Analysis Platform for Mobile Communication

verfasst von: Michael Spranger, Jian Xi, Lukas Jaeckel, Jenny Felser, Dirk Labudde
Erschienen in: KI - Künstliche Intelligenz

Hass im Netz – Aggressivität und Toxizität von Hasskommentaren und Postings, Detektion und Analyse

Christoph Demus, Mina Schütz, Nadine Probol, Jonas Pitz, Melanie Siegel und Dirk Labudde

Danke



labudde@hs-mittweida.de