Science and Technology for Peace and Security

TECHNISCHE UNIVERSITÄT DARMSTADT

Cyber War *und* Cyber Peace:

Schnittmengen der Informatik mit Friedens- und Sicherheitsforschung

Prof. Dr. Dr. **Christian Reuter**

Wissenschaft und Technologie für Frieden und Sicherheit (PEASEC),
Technische Universität Darmstadt

14.11.2024 / Ringvorlesung
„Aktuelle Themen & spannende Entwicklungen in der Cybersicherheit“

HESSEN Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz

Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)

TECHNISCHE UNIVERSITÄT DARMSTADT

… verbindet Informatik mit Friedens- und Sicherheitsforschung

Fokus heute: Schnittmengen der Informatik mit Friedens- und Sicherheitsforschung

In der Schnittmenge der Disziplinen

- **Cyber-Sicherheit und Privatheit**,
- **Friedens- und Konfliktforschung** sowie
- **Mensch-Computer-Interaktion**

adressiert das mehr als 30-köpfige PEASEC-Team besonders folgende Themenbereiche:

(1) Friedensinformatik und technische Friedensforschung
- Cyber-Peace, -War, -Rüstungskontrolle
- Dual Use in der Informatik

(2) Kriseninformatik und Information Warfare
- Soziale Medien und kollaborative Technologien in Konflikt- und Krisenlagen
- Meinungsmanipulation und Fake News

(3) Benutzbare Sicherheit und Privatheit
- Resiliente digitale Infrastrukturen
- Sicherheits- und privatheitsfördernde Maßnahmen

Science and Technology for Peace and Security

TECHNISCHE UNIVERSITÄT DARMSTADT

Desinformationen und Information Warfare

Prof. Dr. Dr. **Christian Reuter**

Wissenschaft und Technologie für Frieden und Sicherheit (PEASEC),
Technische Universität Darmstadt

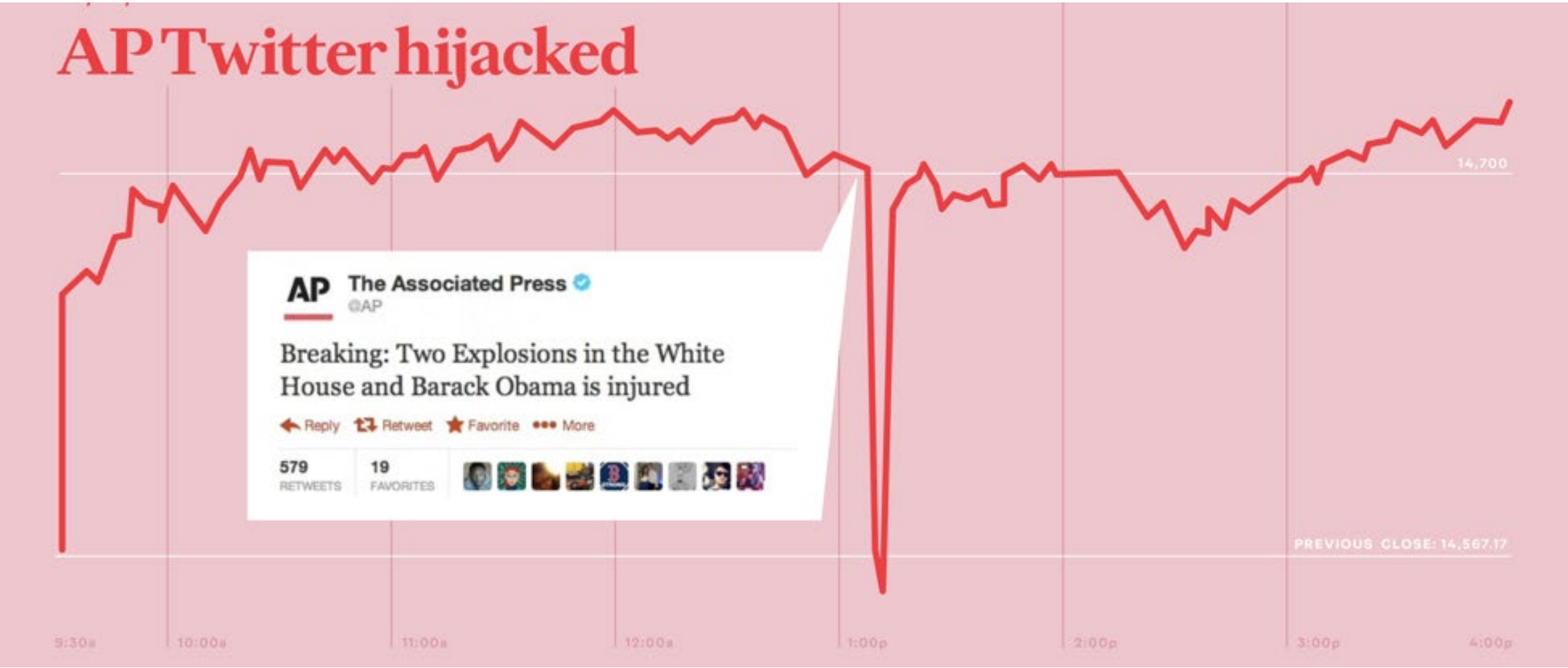
Gefördert innerhalb von:

NEBULA Nutzerzentrierte KI-basierte Erkennung von Fake News und Fehlinformationen

Bundesministerium für Bildung und Forschung

Kostspielige Desinformationen

Desinformationen können schwerwiegende Folgen haben / Finanziell: Aktienindex



Tödliche Desinformationen

Desinformationen in der Corona-Krise über Bleichmittel mit sogar tödlichen Auswirkungen

Verunsichernde Desinformationen

Desinformationen im Kontext von Krieg

Videoclip von lebenden Umweltaktivistinnen und Aktivisten
in Österreich in falschem Kontext verbreitet (snopes.com)

Definitionen von Des-/Misinformationen

Falsch, absichtlich oder nicht?

Desinformationen (auch Fake News)

- Nachrichtenartikel, die **absichtlich** und nachweislich falsch sind und die Lesenden in die Irre führen könnten (Allcott & Gentzkow, 2017)

vs. Misinformationen

- **Unbeabsichtigte** falsche oder ungenaue Informationen, Gerüchte oder Verschwörungstheorien → können genau so viel Schaden anrichten

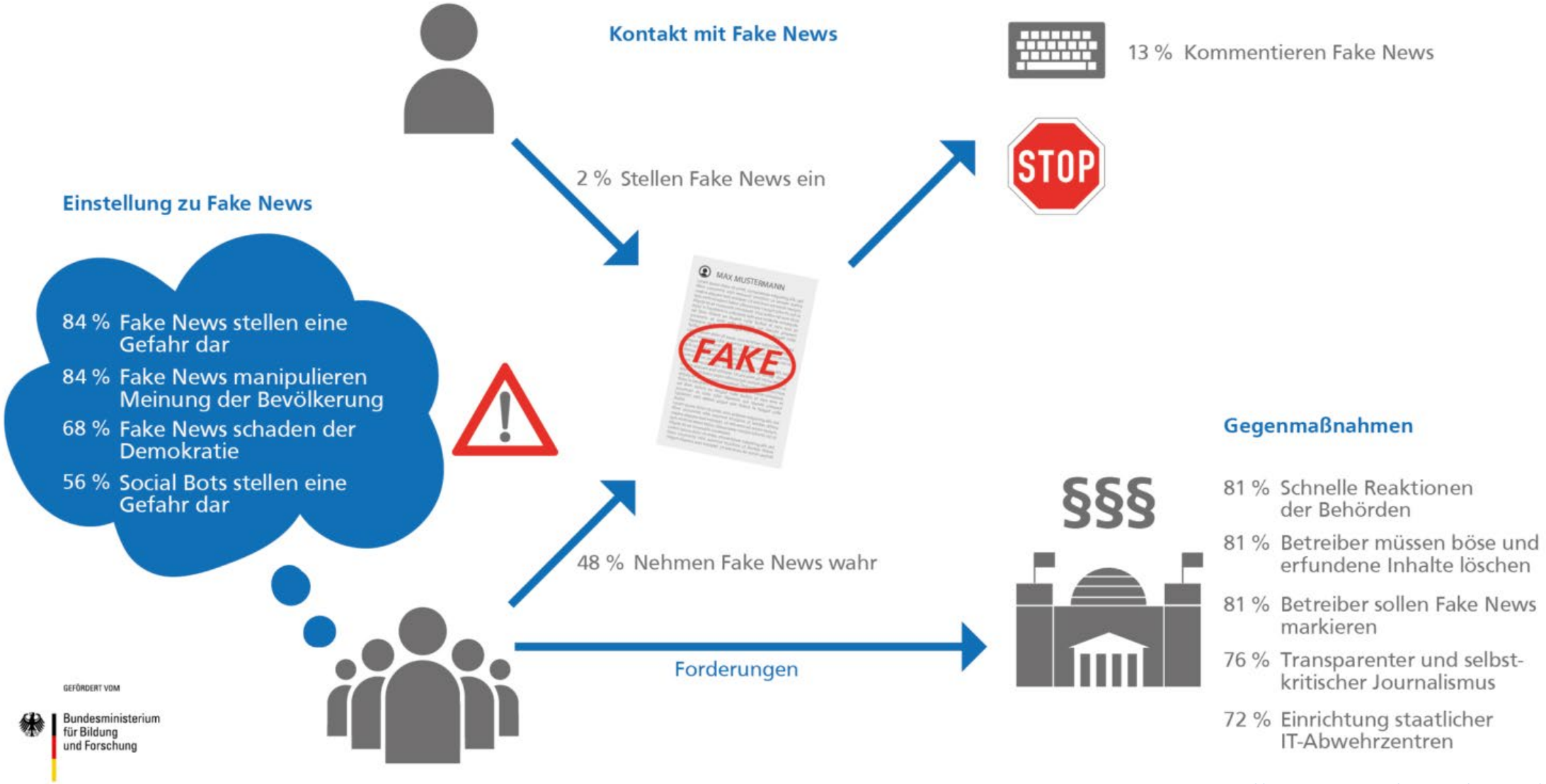
Information Warfare:

- Maßnahmen zur Erlangung von Informationsüberlegenheit durch Manipulation des Gegners und Verteidigung der eigenen Informationen und Medien durch Falschinformationen/teilweise Informationen/Propaganda mit dem **Ziel der Meinungsmanipulation**
  - Nach innen oder nach außen gerichtet (zwischenstaatlich)

Soziale Medien als wichtige Informationsplattformen

- Hohe Geschwindigkeit, niedrige Kosten, (scheinbare) Anonymität, Reziprozität
  - Fördert auch die Verbreitung von Fake News

Teil I: Einstellung in Deutschland



Reuter et al. https://aisel.aisnet.org/wi2019/track09/papers/5/

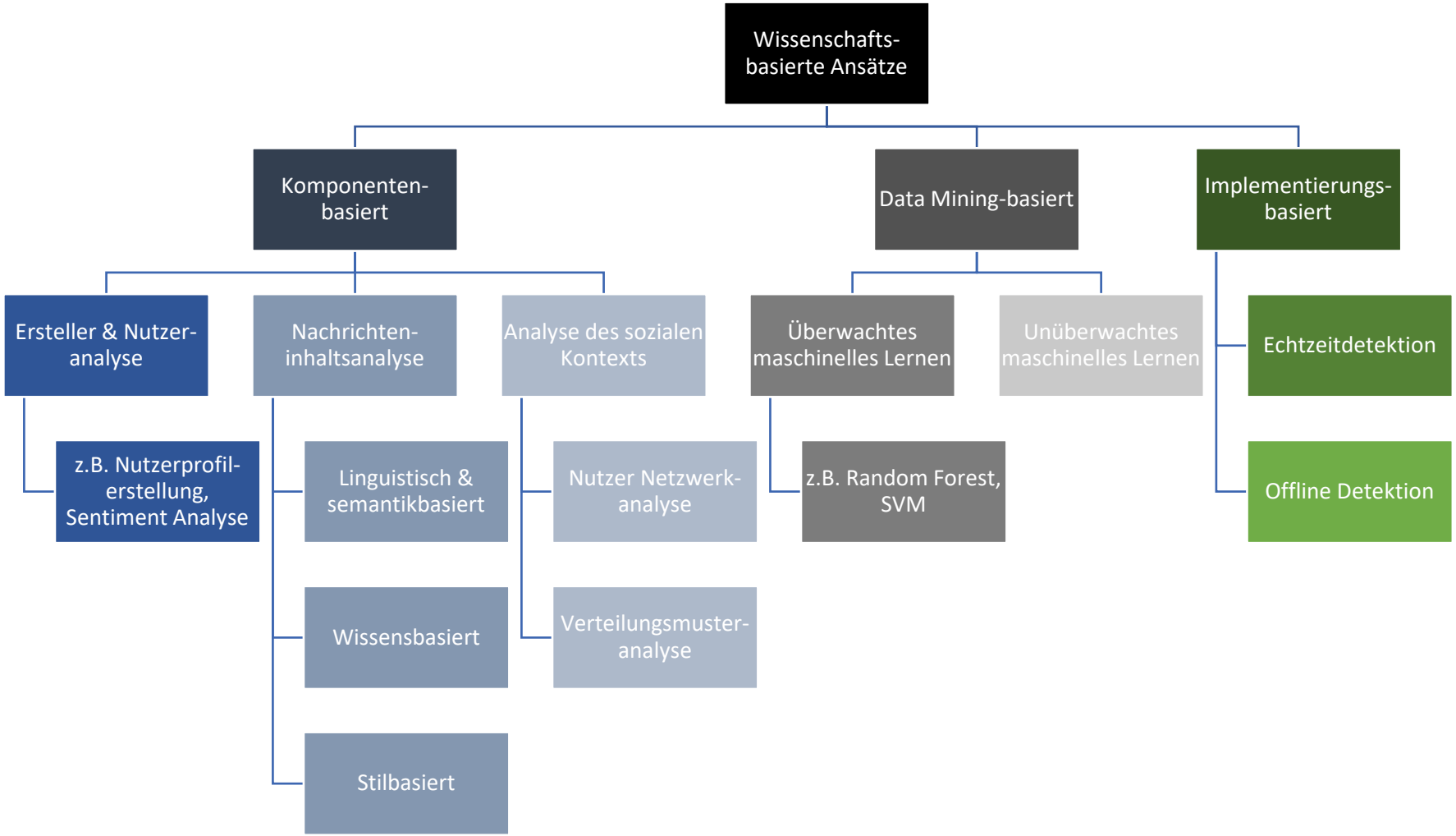
TECHNISCHE UNIVERSITÄT DARMSTADT

Teil II: Effektivität und Akzeptanz von Interventionen

Automatische Erkennung

Erkennung

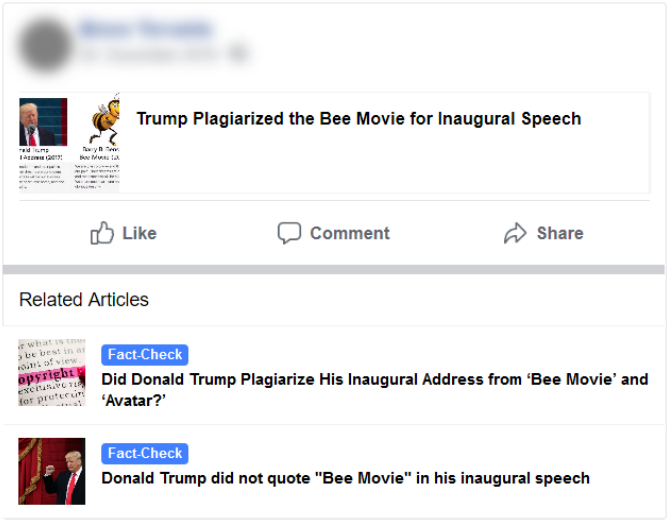
Was dann?
Löschen?
Markieren?



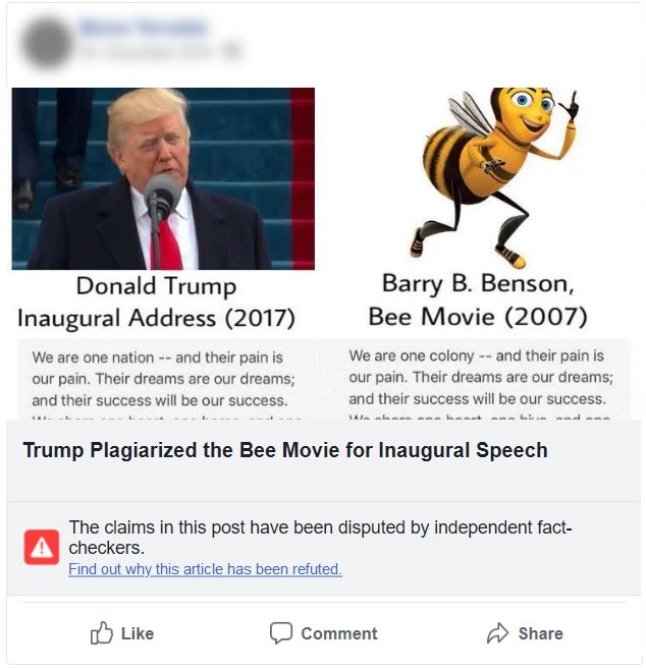
Teil II: Effektivität und Akzeptanz von Interventionen

Nutzerzentrierte Indikatoren

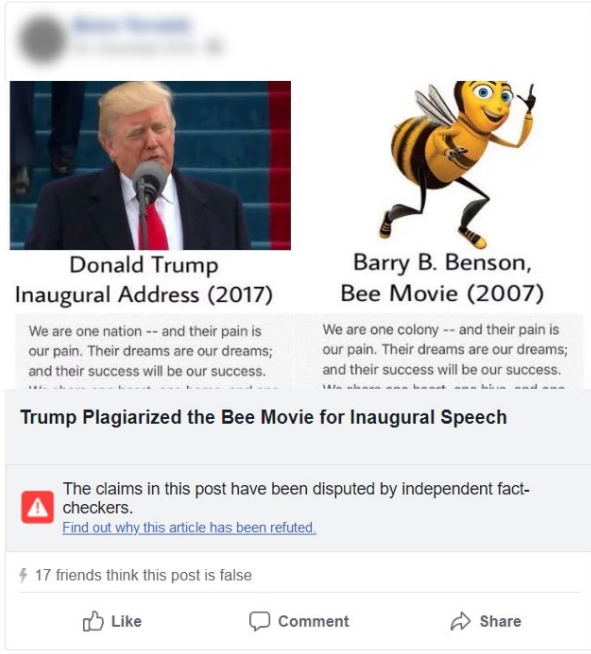
Größe



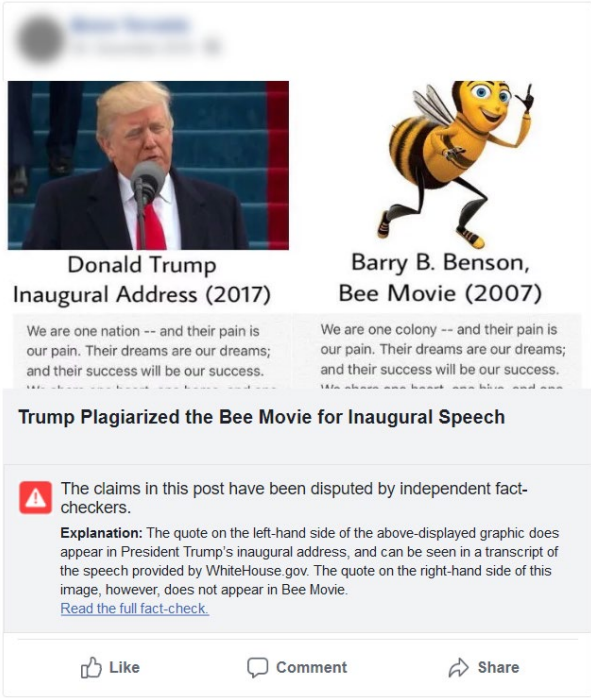
Warnung



Peer / Mitnutzer



Erklärung



Kirchner/Reuter doi:10.1145/3415211

TECHNISCHE UNIVERSITÄT DARMSTADT

Teil II: Effektivität und Akzeptanz von Interventionen

Beispielhafte Falschinformationen

#	Headline	Accuracy	Source
1	Trump Plagiarized the Bee Movie for Inaugural Speech	false	Snopes
2	Man arrested at Berlin Airport with over 10 million euros in cash	false	Correctiv
3	The Icelandic government pays $ 5,000 for every man who marries an Icelandic woman	false	Correctiv
4	Terrifying study: cancer patients die faster with chemotherapy than without treatment	false	Correctiv
5	France passes law saying that children can consent to sex with adults	false	Correctiv
6	Black Friday: The term goes back to the slave trade	false	Correctiv
7	Burglary crime has increased massively in NRW — the clearance rate has stagnated	false	Correctiv
8	Elon Musk leaves Tesla and switches to financial technology	false	Correctiv
9	Trump plans to ban TV shows that promote homosexuality	false	Snopes
10	After curing his own cancer with cannabis, this self-taught doctor healed more than 5,000 patients	false	Correctiv
11	Greens: The liter of gasoline should cost at least 6–7 euros!	false	Correctiv
12	Pentagon wants to have a German warship with them off the Syrian coast	false	Correctiv
13	Croatia donates entire World Cup awards — tough letter to politicians	false	Correctiv
14	Merkel: "Freedom of expression needs strict limits"	false	Correctiv
15	CDU demands pork duty in canteens	false	Mimikama
16	Greens: heating the apartment to 15 degrees is enough	false	Correctiv
17	Hurricane killed and injured in Germany	true	Zeit
18	More asylum seekers live in NRW than in the whole of Italy	true	Correctiv
19	Criminologist: Refugees are reported more often than Germans	true	FAZ
20	Germany earns billions with Greece loans	true	Tagesspiegel
21	Germany pays significantly more child benefit abroad	true	Zeit
22	Palmer demands that violent migrants' freedom of movement be restricted	true	Welt
23	Germany must bring back IS members	true	SZ
24	AfD subsidizes demo participation	true	Correctiv

Table 2. The 24 headlines presented to the participants. Sixteen of which are false and eight are true headlines. While we used German headlines in the study, this table shows their English translation for better intelligibility.

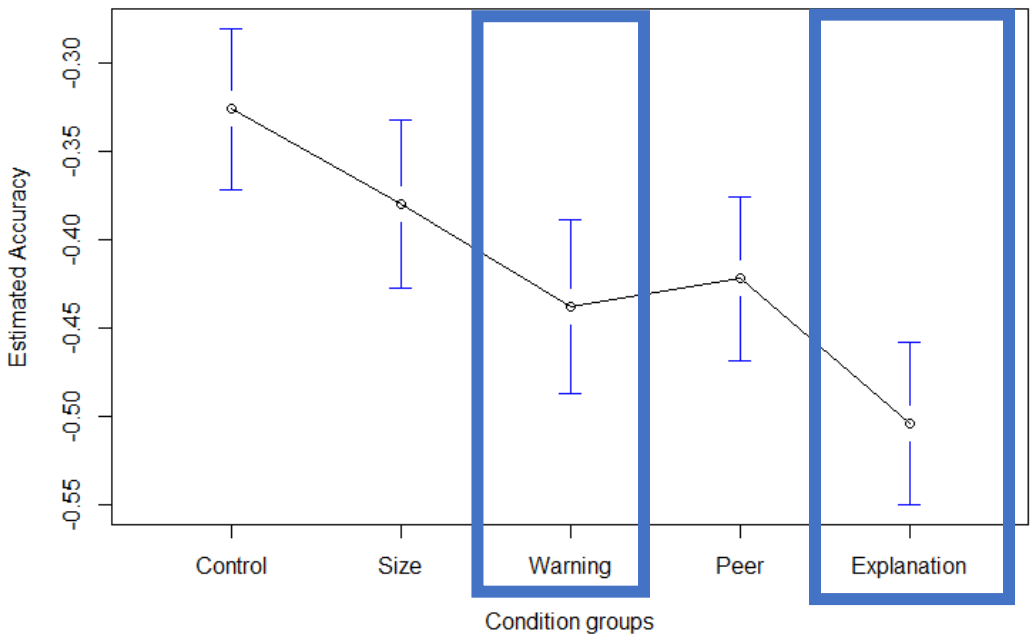
Kirchner/Reuter doi:10.1145/3415211

Teil II: Effektivität und Akzeptanz von Interventionen

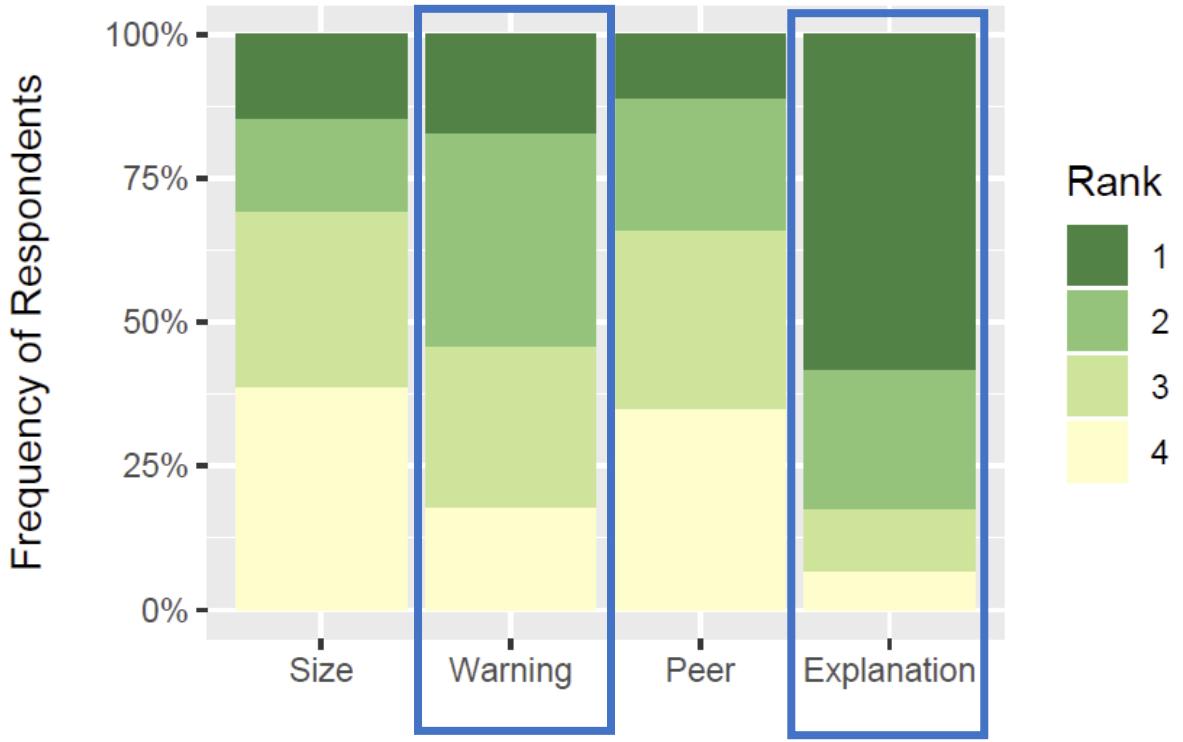
Rangordnung der Gegenmaßnahmen

Effizienz

Durchschnittliche erwartete **Genauigkeit** nach Bedingung



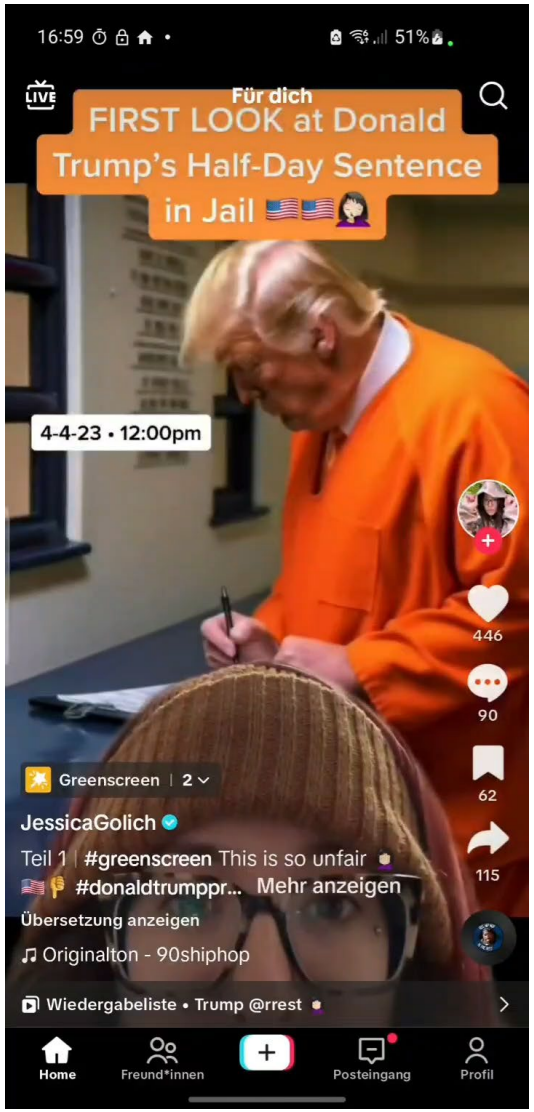
Akzeptanz

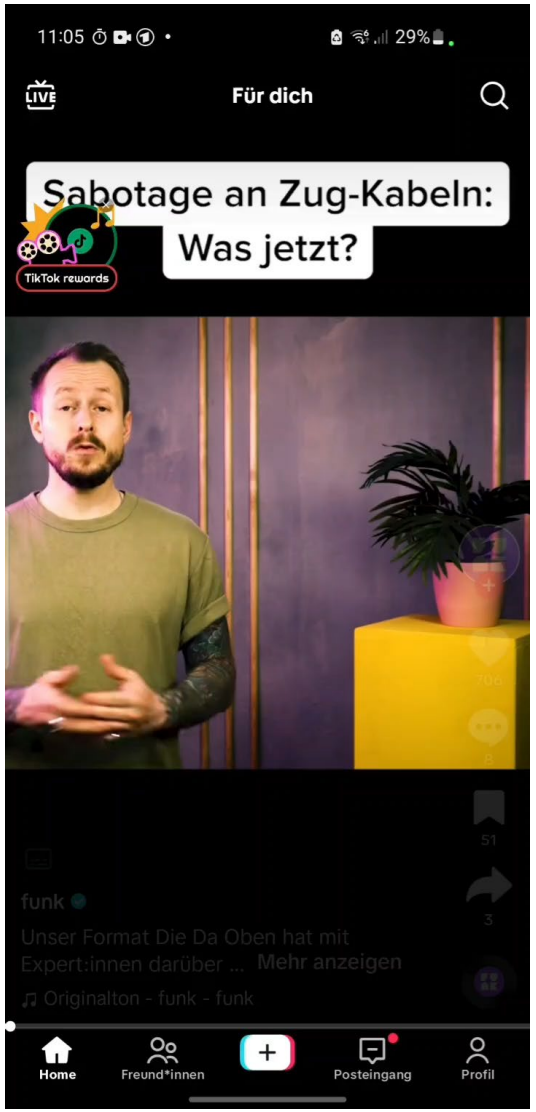


Kirchner/Reuter doi:10.1145/3415211

Teil III: Indikatorbasierte Interventionen

TikTok-Studie mit Jugendlichen: Stimuli



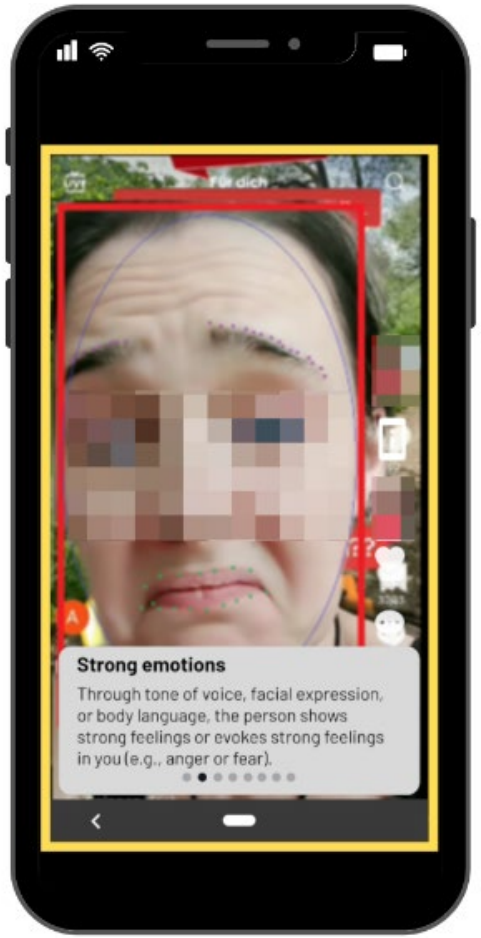


- **Unterschiedlich erfolgreiche Erkennung von Misinformation ohne Hilfestellung**
- **Emotionalisierende Musik / Mimik / Sprache** → wird kaum als manipulierend erkannt
- Bearbeitete Videos erkennen („**Ein Finger zu viel**“ etc.) → Sehr gute Fähigkeiten
- **Video humorvoll oder ironisch** → Erfolgreiche Erkennung
- Sarkasmus oder Ironie als Mittel zur Irreführung → Einige

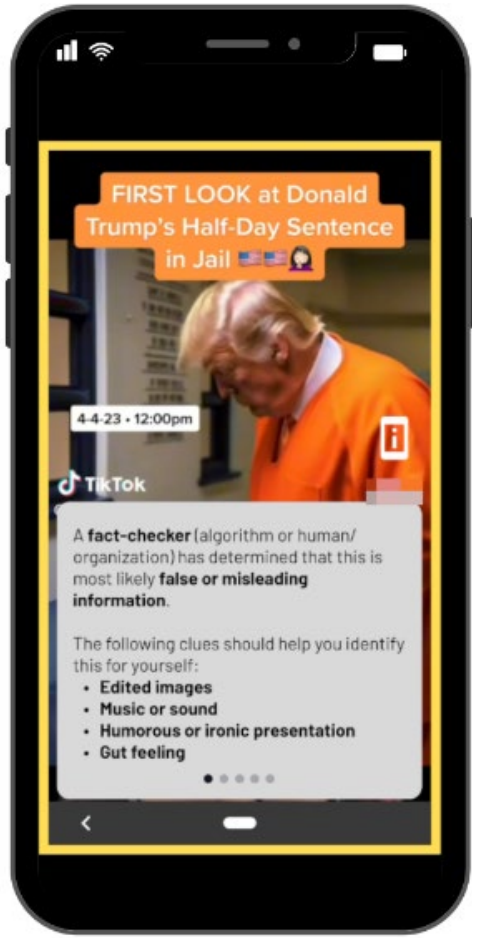
Hartwig et al. doi:10.1145/3613904.3642264

Teil III: Indikatorbasierte Interventionen

TikTok-Studie mit Jugendlichen: Anzeige von Indikatoren

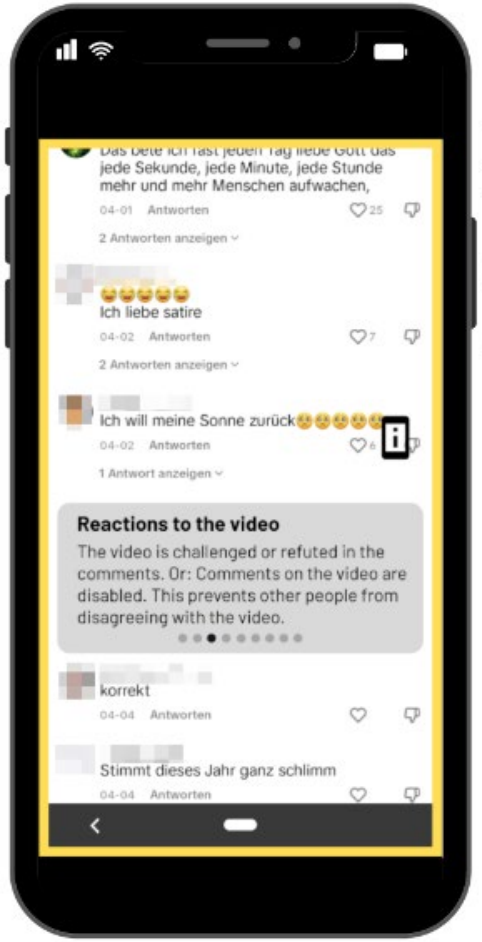


(a) Misinformation



(b) Deep Fake

(c) Satire



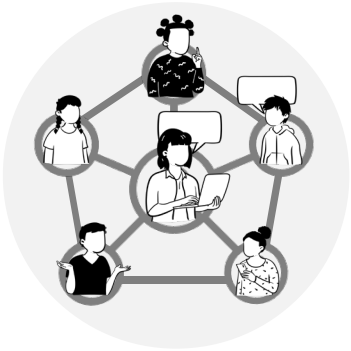
(d) Satire

(e) Wahre Nachrichten

Hartwig et al. doi:10.1145/3613904.3642264

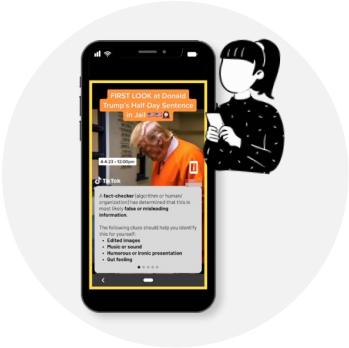
Teil III: Indikatorbasierte Interventionen

Status Quo



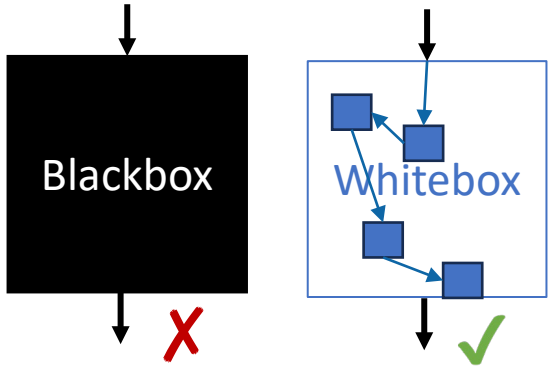
- Jugendliche nutzen **Merkmale von manipulierten Videos**
- Indikatoren auf verschiedenen Ebenen **erweitern und bestätigen** die Wahrnehmungen

Anwendbarkeit des Ansatzes



- **positive Resonanz** auf die indikatorbasierte Anwendung und **gutes Verständnis** ihrer Funktionen

Erfolgsfaktor



- **Transparenz der Indikatoren** für Fehlinformationen sind ein zentraler Grund für die **positive Bewertung** der Intervention

Hartwig et al. doi:10.1145/3613904.3642264

Science and Technology for Peace and Security

TECHNISCHE UNIVERSITÄT DARMSTADT

Cybersicherheit, -Krieg und -Abrüstung

Prof. Dr. Dr. **Christian Reuter**

Wissenschaft und Technologie für Frieden und Sicherheit (PEASEC),
Technische Universität Darmstadt

Gefördert innerhalb von:
ATHENE Nationales Forschungszentrum für angewandte Cybersicherheit
CY-WARN Cyber Situational Awareness & Communication
CROSSING Privacy and Trust for Mobile Users
HESSEN Hessisches Ministerium für Wissenschaft und Kunst
Bundesministerium für Bildung und Forschung
DFG

Cybersicherheits-Lage und -Lagebild

- **Cybersecurity-Kommunikation** im Fokus
  - Informationsgewinnung aus Social Media, Datenbanken, Hersteller-Webseiten, etc.
  - Analyse der Informationen
  - Effektive Kommunikation/Verbreitung
    - **Cyber Threat Intelligence (CTI)**

Mehr als **2.000** Schwachstellen in Software produkten (15% davon kritisch) wurden [..] durchschnittlich **im Monat** bekannt.

Eine Viertelmillion
neue **Schadprogramm-Varianten** wurden durchschnittlich **an jedem Tag** [..] gefunden.

Die Lage der IT-Sicherheit in Deutschland 2023, BSI

- Langjährige Studie mit **Länder-CERTs**
  - CERTs verbringen **täglich mehrere Stunden** mit **Monitoring** von Cybersecurity-Kommunikation
  - **Informationsüberfluss**

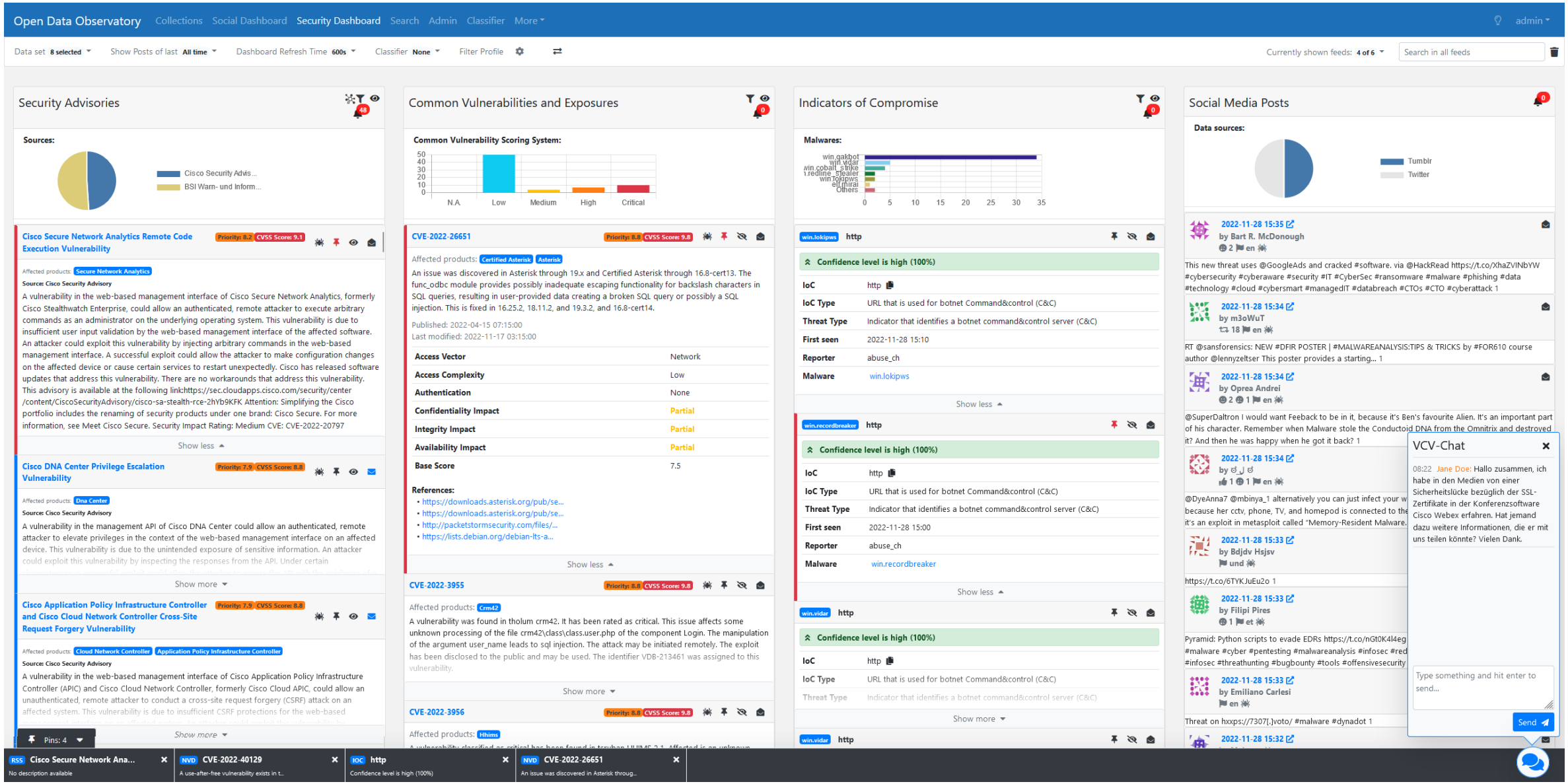
> “
> Derzeit haben wir nicht die Kapazitäten, um alle Medien zu überwachen. Wir würden von einem **höheren Grad an Automatisierung profitieren** [..]
> - CERT Incident Manager

> “
> Die manuelle Bearbeitung kann überwältigend sein. Die Menge kann zu einer **Informationsüberflutung** führen und wichtige Details können übersehen werden. **Automatisierung würde uns erheblich helfen** [..]
> - CERT Incident Manager

Übersetzt aus (Kaufhold, Riebe, Bayer, Reuter, 2024)

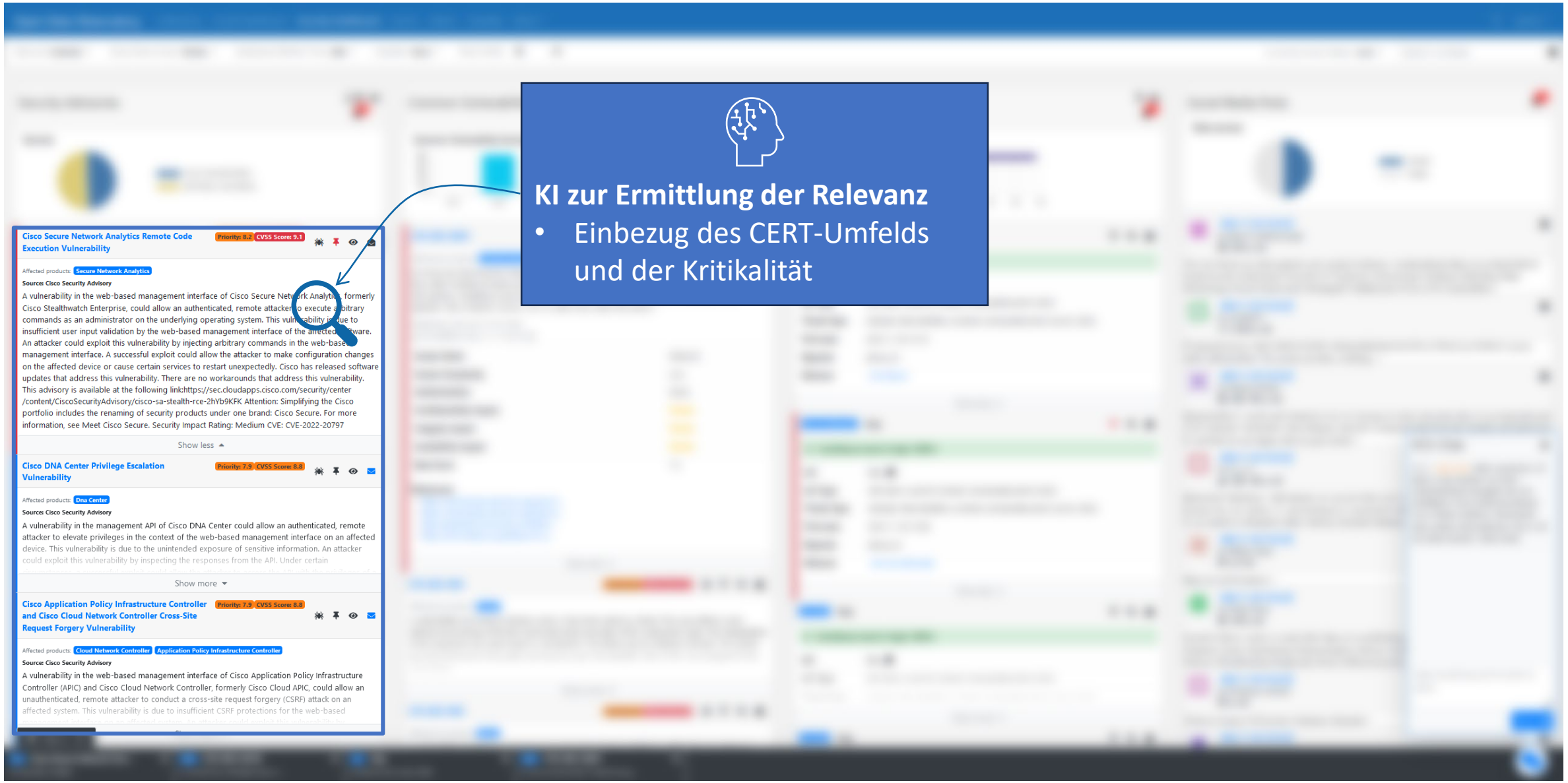
Kaufhold et al. http://dx.doi.org/10.1145/3613904.3642368

Cybersicherheits-Lagebild: Open Data Observatory



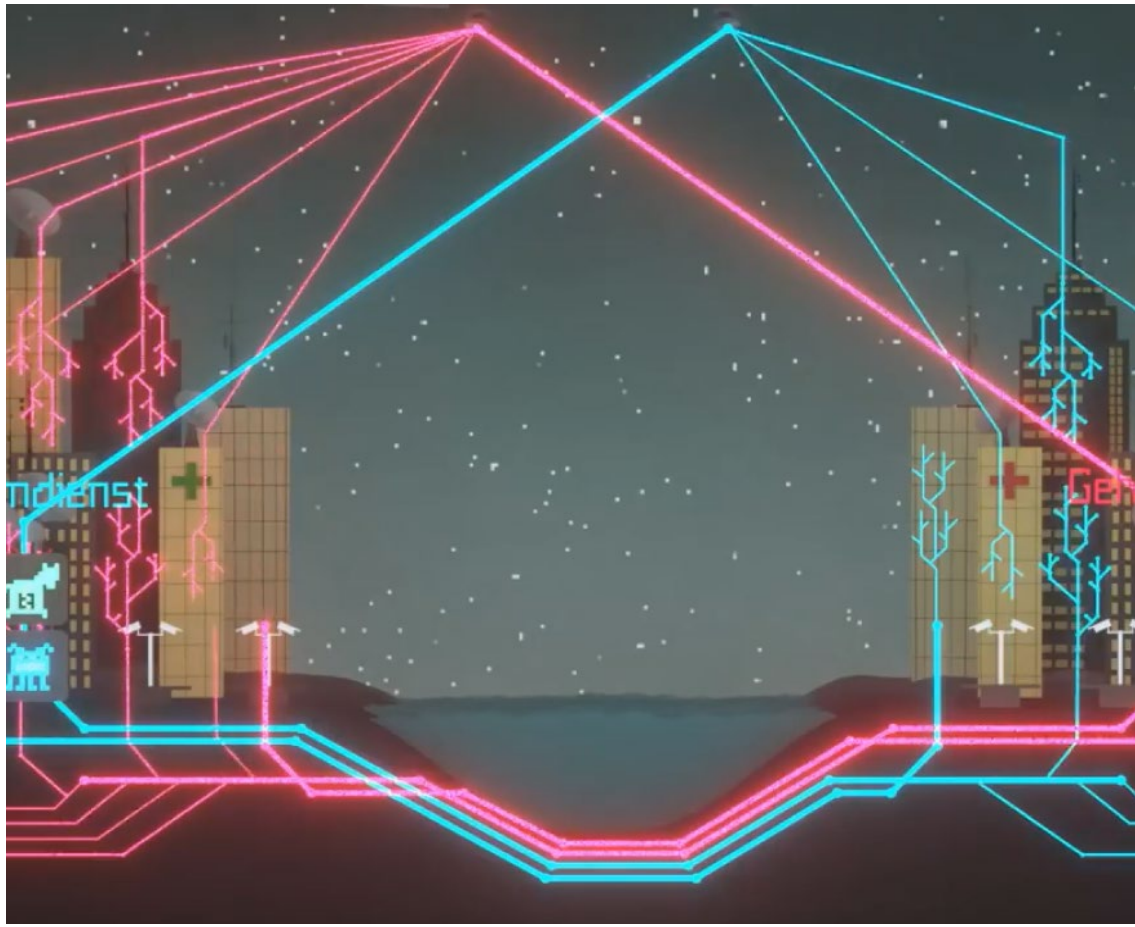
Kaufhold et al. http://dx.doi.org/10.1145/3613904.3642368

Cybersicherheits-Lagebild: Open Data Observatory



Cyberwaffen, staatliche Akteure und Abrüstung

- Man kennt **konventionelle Kriegsführung**
- Was ist Information vs. **Cyber Warfare**
  - **Cyberwaffen:** „Grundmaterial“ sind Sicherheitslücken
  - Bedrohungen durch nicht-veröffentlichte Sicherheitslücken
- Was machen **Staaten im Cyberspace**?
  - Kaufen und Sammeln von Schwachstellen
  - sog. **Vulnerability Stockpiles**
- Zentrale Frage:
  - Generell: **Wie kann Cyber-Abrüstung erfolgen?**
  - Konkret: **Wie können Vulnerability Stockpiles zwischen Staaten abgebaut werden**?
- Forschungslücke:
  - **Verfahren zur Stockpile-Reduktion zwischen nicht-vertrauensvollen Akteuren**



Source: https://youtu.be/St955HBD-7k

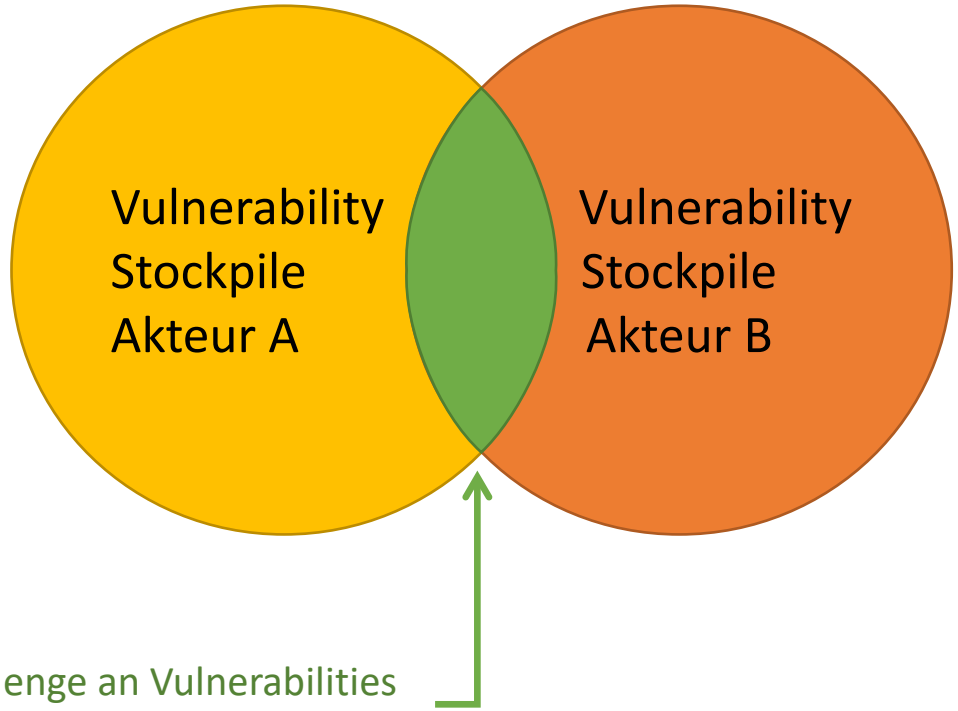
Abbau der Schwachstellenvorräte der Staaten

TECHNISCHE UNIVERSITÄT DARMSTADT

mit ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

- **Prämisse**:
  - Mehrfach bekannte Sicherheitslücke kann nicht mehr eingesetzt werden, weil Gegner darauf vorbereitet ist
  - Freigabe dieser Sicherheitslücken zur Veröffentlichung ist ein eigennütziger Sicherheitsgewinn für beteiligte Akteure

- **Anforderungsanalyse**:
  - Verfahren muss **ohne** gegenseitiges **Vertrauen** funktionieren
  - **Kein Offenlegen** von Geheimnissen jeglicher Art
  - **Gehärtet** gegen „malicious (active) adversaries“ (bis zu N-1)
  - **Keine neutrale Instanz** nötig
  - Übermittelte Daten **nicht** nachträglich **veränderbar**
  - **Vermeidung falsch-positiver** Ergebnisse



https://www.pexels.com/de-de/foto/full-house-card-anzug-2555292/

Reinhold et al. http://dx.doi.org/10.1109/TTS.2023.3280356

Technische Lösungen für Cyberabrüstung

TECHNISCHE UNIVERSITÄT DARMSTADT

mit ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Schritt 1: Eindeutiger maschineller Vergleich

- **Maschineller Vergleich** erfordert **eindeutige Beschreibbarkeit von Schwachstellen**
  - Ziel: Methodik, bei der unterschiedliche Akteure die gleiche Schwachstelle gleich beschreiben
- **Grundlage: National Vulnerability Database** (NVD)
  - Entfernung Freieingaben und unnötiger, uneindeutiger Angaben
  - Hinzufügen von Informationen über den vulnerablen Code-Bestandteil (z.B. Funktionsnamen)
  - Zusätzliche Angaben von CWE-Klassen (Common Weakness Enumeration) und der Common Platform Enumeration (CPE)

```
{
  "cpe": "cpe:2.3:o:tp-link:wdr7400_firmware:-:*:*:*
      ↪ :*:*:*:*",
  "cwe": 120,
  "fun": "copy_msg_element"
}
```

Listing 1. Vulnerability Identifier for CVE-2020-28877

Schritt 2: Berechnung/Abgleich

- Basierend auf **interactive MultiParty Computation** (MPC)
  - n Akteure berechnen vereinbarte Funktion *f* auf ihren jeweiligen geheimen Eingaben *x1, . . . , xN*
  - Austausch des berechneten Ergebnis *f(x1, . . . , xN)*
- Abgleich der Ergebnisse *f(x1, . . . , xN)* über Private Set Intersection (PSI) Algorithmus
- Akteur erhält Information darüber, ob/welche seiner Eingaben eine Kollision erzeugt haben

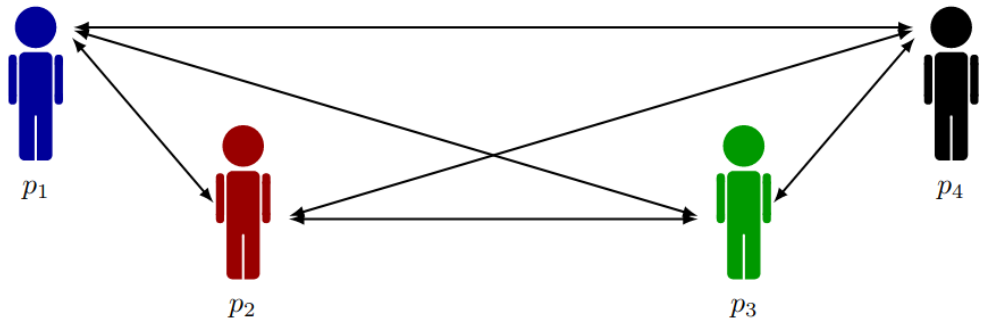


Fig. 2. MPC setting with four participating parties $p_1, \ldots, p_4$.

Reinhold et al. http://dx.doi.org/10.1109/TTS.2023.3280356

Technische Lösungen für Cyberabrüstung (ExTRUST)

Datenschutzfreundliches Depletion-System für zwischenstaatliche Beziehungen

mit ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

Wie können Maßnahmen zur Deeskalation von staatlich geführten Konflikten im Cyberspace und für die Rüstungskontrolle von Cyberwaffen entwickelt werden?

- Ergebnisse und Beitrag:
  - Schema zur eindeutigen Beschreibung von Exploits
  - ExTRUST zum Abgleich von Vulnerability-Stockpiles, **ohne Notwendigkeit einer neutralen Instanz**
  - Keine Offenlegung von Informationen über verglichene Vulnerabilities oder identifizierte Kollisionen an Dritte
- Limitierungen:
  - Skalierbar bis n ≈ 10 bei einer Komplexität $O(N^2)$
  - Abgleich erfordert Kooperation
  - Technische Sicherheit vs. politisches Handeln von Staaten

ExTRUST: Reducing Exploit Stockpiles with a Privacy-Preserving Depletion System for Inter-State Relationships

Thomas Reinhold*, Philipp Kuehn*, Daniel Günther†, Thomas Schneider† and Christian Reuter*
*Science and Technology for Peace and Security (PEASEC)
Technical University of Darmstadt, Germany
†Cryptography and Privacy Engineering (ENCRYPTO)
Technical University of Darmstadt, Germany

Reinhold et al. http://dx.doi.org/10.1109/TTS.2023.3280356

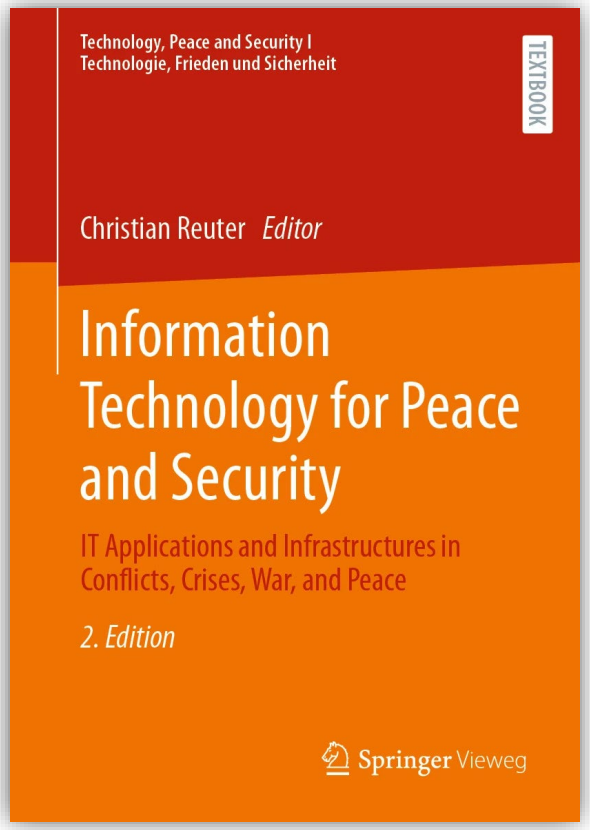
Ausblick

Prof. Dr. Dr. **Christian Reuter**

Wissenschaft und Technologie für Frieden und Sicherheit (PEASEC),
Technische Universität Darmstadt

Buch: Informationstechnologie für Frieden und Sicherheit

IT Applications and Infrastructures in Conflicts, Crises, War, and Peace (Springer Vieweg)



Erschienen: **1.11.2024**
in 2. überarbeiteter Auflage

Erstauflage: 2019

- Explores the history and dangerous future of unchecked information warfare
- Describes efforts to promote cyber arms control by building trust and transparency
- Establishes a new research direction: **information technology for peace and security**

Reuter (2024): Information Technology for Peace and Security – *IT Applications and Infrastructures in Conflicts, Crises, War, and Peace;* https://doi.org/10.1007/978-3-658-44810-3; eBook ISBN: 978-3-658-44810-3

Part I: Fundamentals
- 1: An Overview and Introduction / Reuter et al.
- 2: Peace Informatics / Reuter et al.
- 3: Natural Science/Technical Peace Research / Altmann

Part II: Cyber Conflicts and War
- 4: Information Warfare / Ruhmann/Bernhardt
- 5: Cyber Espionage and Cyber Defence / Herrmann
- 6: Darknets and Civil Security / Denker et al.

Part III: Cyber Peace
- 7: From Cyber War to Cyber Peace / Reinhold, Reuter
- 8: Dual-Use Information Technology / Riebe et al.
- 9: Confidence and Security Building Measures for Cyber Forces / Altmann

Part IV: Cyber Arms Control
- 10: Arms Control and Its Applicability to Cyberspace / Reinhold/Reuter
- 11: Verification in Cyberspace / Reinhold/Reuter
- 12: Attribution of Cyber Attacks / Saalbach

Part V: Cyber Infrastructures
- 13: Secure Critical Infrastructures / Franken/Reuter
- 14: Resilient Critical Infrastructures / Hollick/Katzenbeisser
- 15: Information Infrastructures / Dehling et al.

Part VI: Artificial Intelligence
- 16: Artificial Intelligence and Cyber Weapons / Reinhold/Reuter
- 17: Unmanned Systems / Schörnig

Part VII: ICT in Peace and Conflict
- 18: Cultural Violence in Social Media / Kaufhold et al.
- 19: Political Activism in Conflict and War / Aal et al.
- 20: Digital Peacebuilding and PeaceTech / Schirch

Part VIII: Outlook
- 21: Teaching Peace Informatics / Reuter et al.
- 22: Outlook: The Future of IT in Peace and Security / Reuter et al.

Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)

TECHNISCHE UNIVERSITÄT DARMSTADT

… verbindet Informatik mit Friedens- und Sicherheitsforschung

In der Schnittmenge der Disziplinen

- **Cyber-Sicherheit und Privatheit**,
- **Friedens- und Konfliktforschung** sowie
- **Mensch-Computer-Interaktion**

adressiert das mehr als 30-köpfige PEASEC-Team besonders folgende Themenbereiche:

(1) Friedensinformatik und technische Friedensforschung
- Cyber-Peace, -War, -Rüstungskontrolle
- Dual Use in der Informatik

(2) Kriseninformatik und Information Warfare
- Soziale Medien und kollaborative Technologien in Konflikt- und Krisenlagen
- Meinungsmanipulation und Fake News

(3) Benutzbare Sicherheit und Privatheit
- Resiliente digitale Infrastrukturen
- Sicherheits- und privatheitsfördernde Maßnahmen

Science and Technology for Peace and Security

TECHNISCHE UNIVERSITÄT DARMSTADT

Cyber War *und* Cyber Peace:

Schnittmengen der Informatik mit Friedens- und Sicherheitsforschung

Prof. Dr. Dr. **Christian Reuter**

Wissenschaft und Technologie für Frieden und Sicherheit (PEASEC),
Technische Universität Darmstadt

14.11.2024 / Ringvorlesung
„Aktuelle Themen & spannende Entwicklungen in der Cybersicherheit“

HESSEN Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz

Zentrale Quellen

Abrufbar unter https://peasec.de/publications/

- Reuter, Christian, Katrin Hartwig, Jan Kirchner, und Noah Schlegel. „Fake News Perception in Germany: A Representative Study of People's Attitudes and Approaches to Counteract Disinformation". In *Proceedings of the International Conference on Wirtschaftsinformatik (WI)*, 1069–83. Siegen, Germany: AIS, 2019. http://www.peasec.de/paper/2019/2019_ReuterHartwigKirchnerSchlegel_FakeNewsPerceptionGermany_WI.pdf.
- Hartwig, Katrin, Frederic Doell, und Christian Reuter. „The Landscape of User-centered Misinformation Interventions – A Systematic Literature Review". *ACM Computing Surveys (CSUR)* 56, Nr. 11 (Juli 2024). https://doi.org/10.1145/3674724.
- Kirchner, Jan, und Christian Reuter. „Countering Fake News: A Comparison of Possible Solutions Regarding User Acceptance and Effectiveness". *Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing* 4, Nr. CSCW2 (2020): 140:1-140:28. https://doi.org/10.1145/3415211.
- Hartwig, Katrin, Tom Biselli, Franziska Schneider, und Christian Reuter. „From Adolescents' Eyes: Assessing an Indicator-Based Intervention to Combat Misinformation on TikTok". In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. CHI '24. New York, NY, USA: Association for Computing Machinery, 2024. https://doi.org/10.1145/3613904.3642264.
- Bayer, Markus, Philipp Kuehn, Ramin Shanehsaz, und Christian Reuter. „CySecBERT: A Domain-Adapted Language Model for the Cybersecurity Domain". *ACM Transactions on Privacy and Security (TOPS)* 27, Nr. 2 (April 2024). https://doi.org/10.1145/3652594.
- Kaufhold, Marc-André, Thea Riebe, Markus Bayer, und Christian Reuter. „‚We Do Not Have the Capacity to Monitor All Media': A Design Case Study on Cyber Situational Awareness in Computer Emergency Response Teams". In *Proceedings of the Conference on Human Factors in Computing Systems (CHI) (Best Paper Award)*. CHI '24. New York, NY, USA: Association for Computing Machinery, 2024. https://doi.org/10.1145/3613904.3642368.
- Reinhold, Thomas, Philipp Kuehn, Daniel Günther, Thomas Schneider, und Christian Reuter. „ExTRUST: Reducing Exploit Stockpiles With a Privacy-Preserving Depletion Systems for Inter-State Relationships". *IEEE Transactions on Technology and Society* 4, Nr. 2 (2023): 158–70. https://doi.org/10.1109/TTS.2023.3280356.