



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)

... 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



**Fokus heute:
Schnittmengen der
Informatik
mit Friedens- und
Sicherheitsforschung**

① PEASEC | ② Information Warfare | ③ Cyber Warfare | ④ Ausblick

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



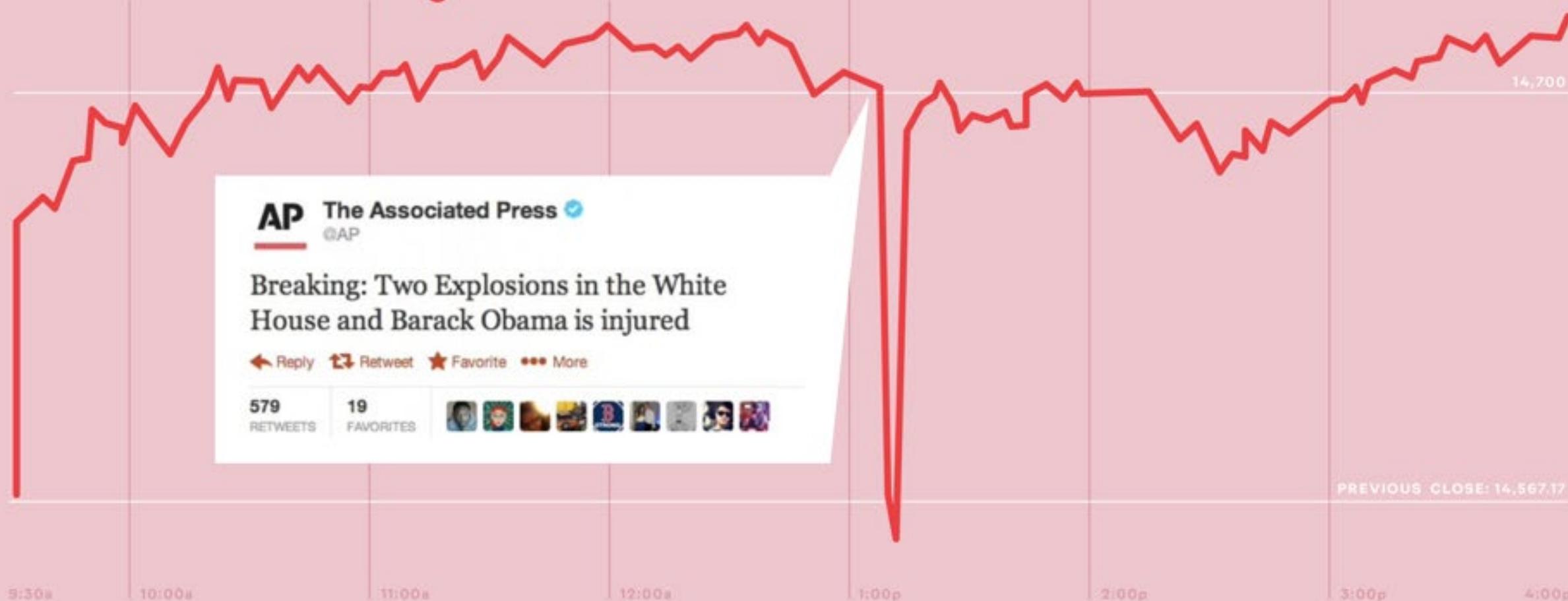
Bundesministerium
für Bildung
und Forschung



Kostspielige Desinformationen

Desinformationen können schwerwiegende Folgen haben / Finanziell: Aktienindex

AP Twitter hijacked



Tödliche Desinformationen

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



Verunsichernde Desinformationen

Desinformationen im Kontext von Krieg



WIEN: DEMO GEGEN KLIMAPOLITIK



**UKRAINIAN HEALTH MINISTRY: 57 DEAD, 169 H
ACROSS UKRAINE AS RUSSIA LAUNCHES ATTA**

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:

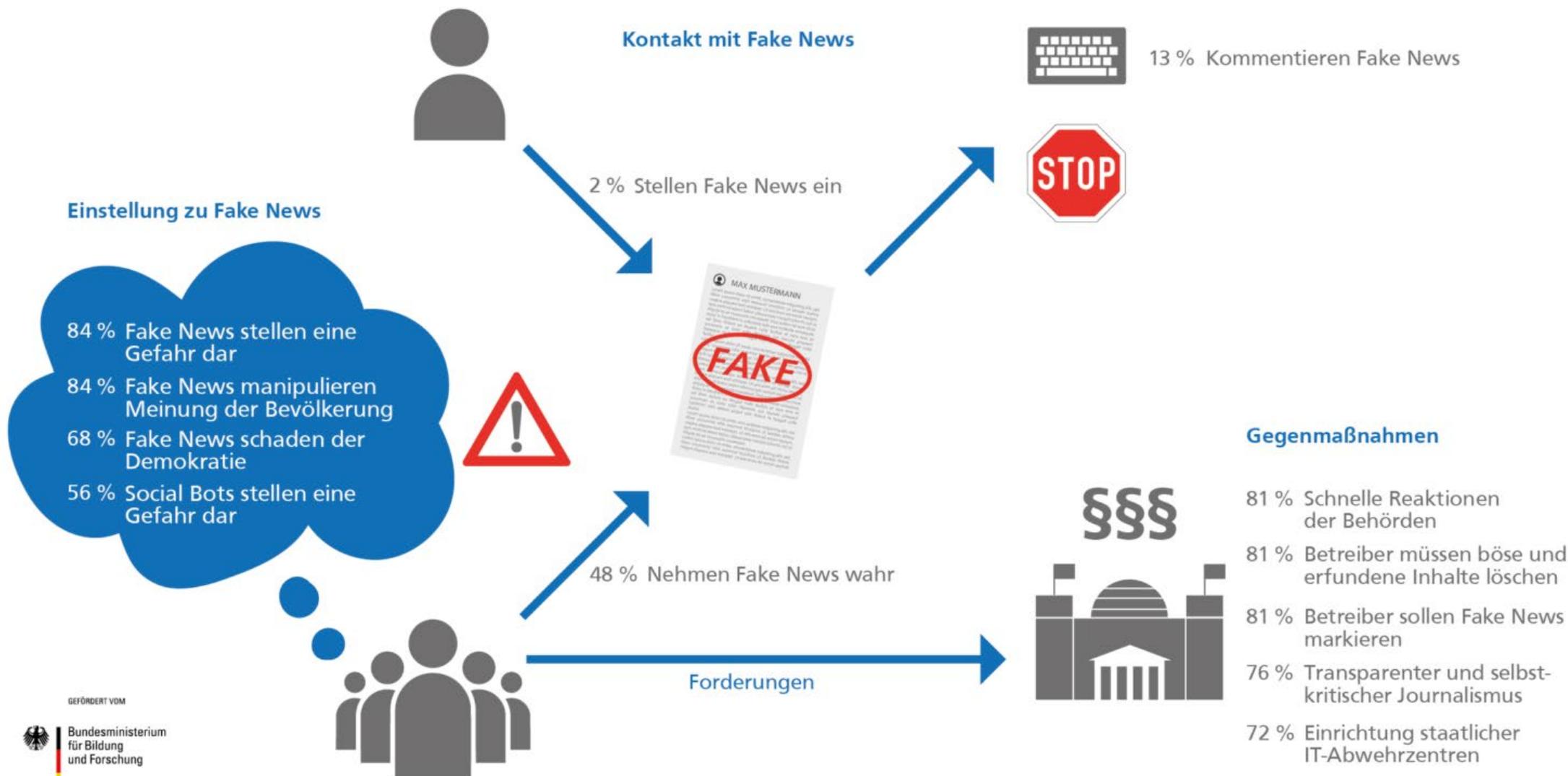
- Maßnahmen zur Erlangung von Informationsüberlegenheit durch Manipulation des Gegners und Verteidigung der eigenen Informationen und Medien durch Falschinformationen/teilweise Informationen/Propaganda mit dem **Ziel der Meinungsmanipulation**
 - Nach innen oder nach außen gerichtet (zwischenstaatlich)

Soziale Medien als wichtige Informationsplattformen

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



Teil I: Einstellung in Deutschland



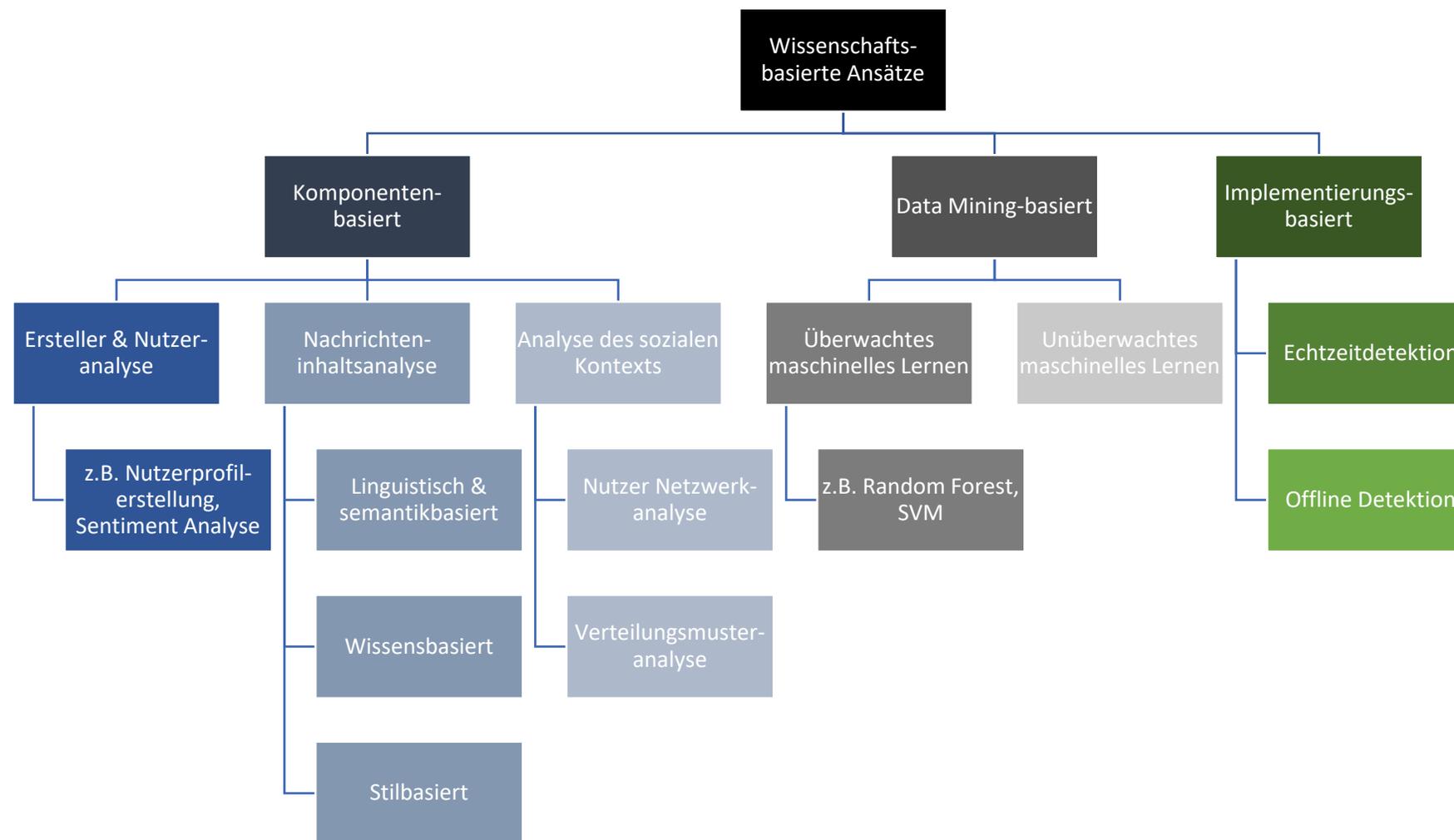
Teil II: Effektivität und Akzeptanz von Interventionen

Automatische Erkennung

Erkennung



Was dann?
Löschen?
Markieren?



Teil II: Effektivität und Akzeptanz von Interventionen

Nutzerzentrierte Indikatoren

Größe

Trump Plagiarized the Bee Movie for Inaugural Speech

Like Comment Share

Related Articles

Fact-Check
Did Donald Trump Plagiarize His Inaugural Address from 'Bee Movie' and 'Avatar'?

Fact-Check
Donald Trump did not quote "Bee Movie" in his inaugural speech

Warnung

Donald Trump Inaugural Address (2017)

Barry B. Benson, Bee Movie (2007)

We are one nation -- and their pain is our pain. Their dreams are our dreams; and their success will be our success.

We are one colony -- and their pain is our pain. Their dreams are our dreams; and their success will be our success.

Trump Plagiarized the Bee Movie for Inaugural Speech

Warning: The claims in this post have been disputed by independent fact-checkers.
[Find out why this article has been refuted.](#)

Like Comment Share

Peer / Mitnutzer

Donald Trump Inaugural Address (2017)

Barry B. Benson, Bee Movie (2007)

We are one nation -- and their pain is our pain. Their dreams are our dreams; and their success will be our success.

We are one colony -- and their pain is our pain. Their dreams are our dreams; and their success will be our success.

Trump Plagiarized the Bee Movie for Inaugural Speech

Warning: The claims in this post have been disputed by independent fact-checkers.
[Find out why this article has been refuted.](#)

⚡ 17 friends think this post is false

Like Comment Share

Erklärung

Donald Trump Inaugural Address (2017)

Barry B. Benson, Bee Movie (2007)

We are one nation -- and their pain is our pain. Their dreams are our dreams; and their success will be our success.

We are one colony -- and their pain is our pain. Their dreams are our dreams; and their success will be our success.

Trump Plagiarized the Bee Movie for Inaugural Speech

Warning: The claims in this post have been disputed by independent fact-checkers.

Explanation: The quote on the left-hand side of the above-displayed graphic does appear in President Trump's inaugural address, and can be seen in a transcript of the speech provided by WhiteHouse.gov. The quote on the right-hand side of this image, however, does not appear in Bee Movie.
[Read the full fact-check.](#)

Like Comment Share

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

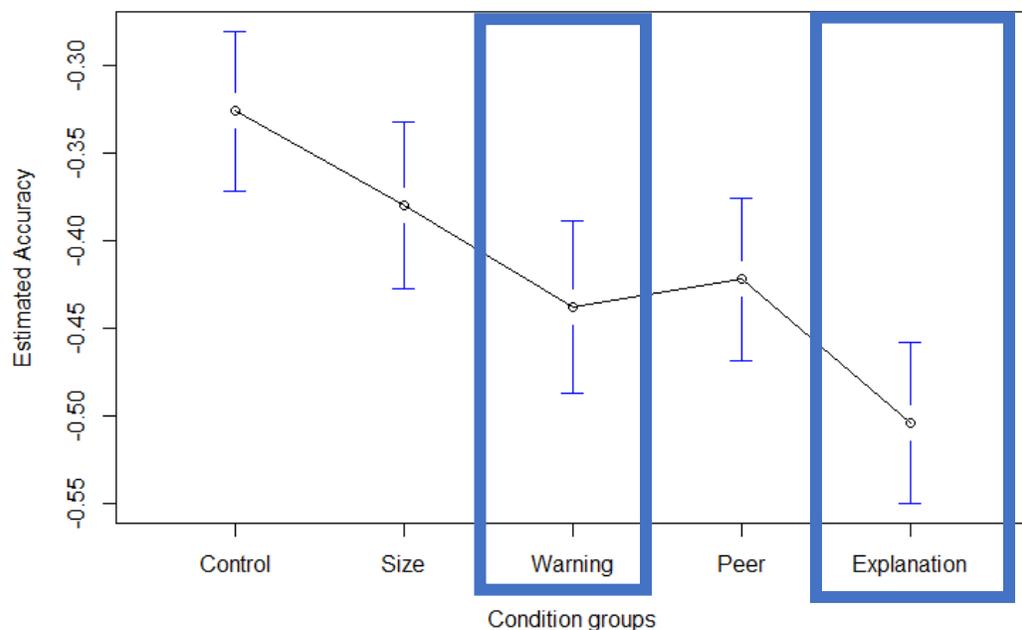
Table 2. The 24 headlines presented to the participants. Sixteen of which are false and eight are true headlines. While we used German headlines in the study, this table shows their English translation for better intelligibility.

Teil II: Effektivität und Akzeptanz von Interventionen

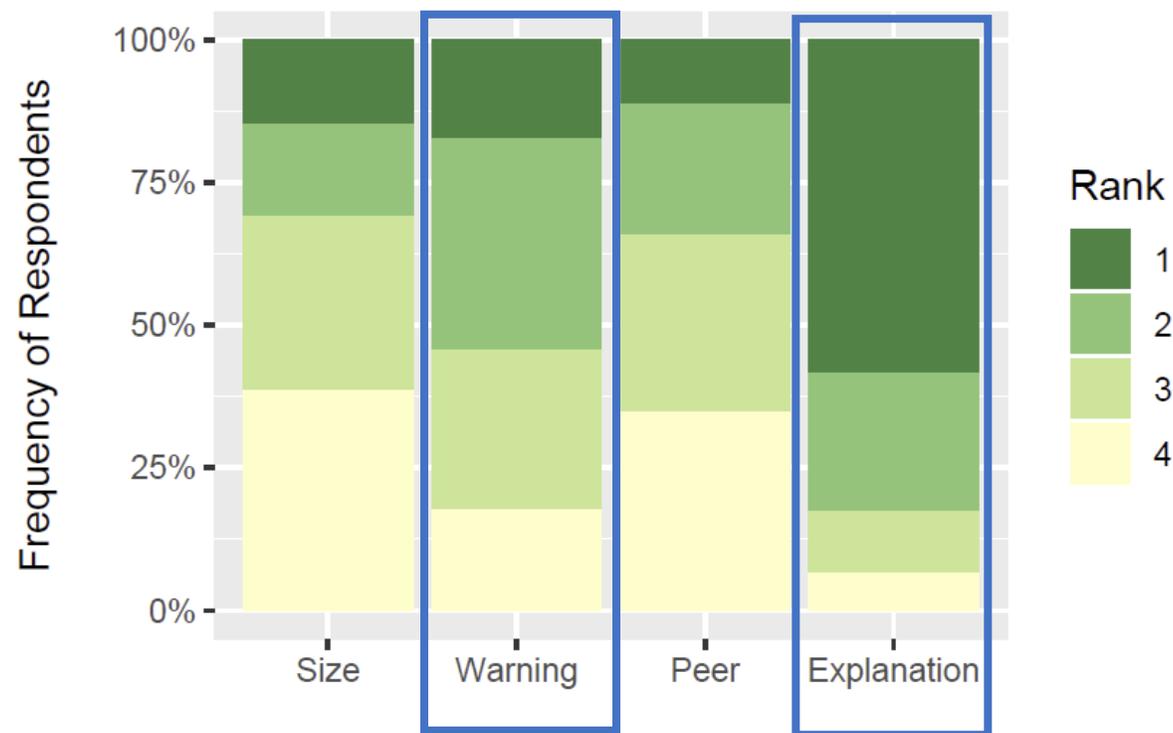
Rangordnung der Gegenmaßnahmen

Effizienz

Durchschnittliche erwartete Genauigkeit nach Bedingung

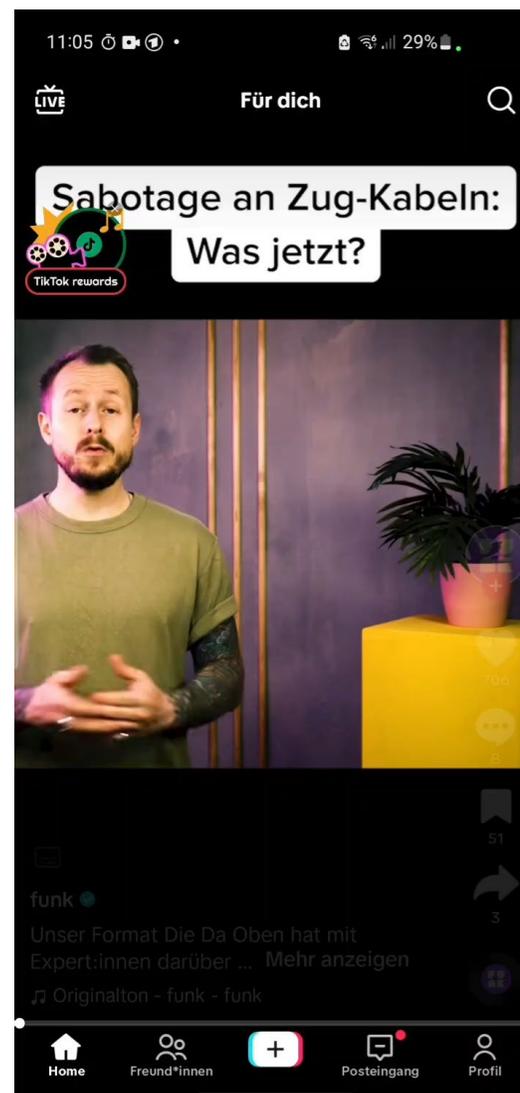
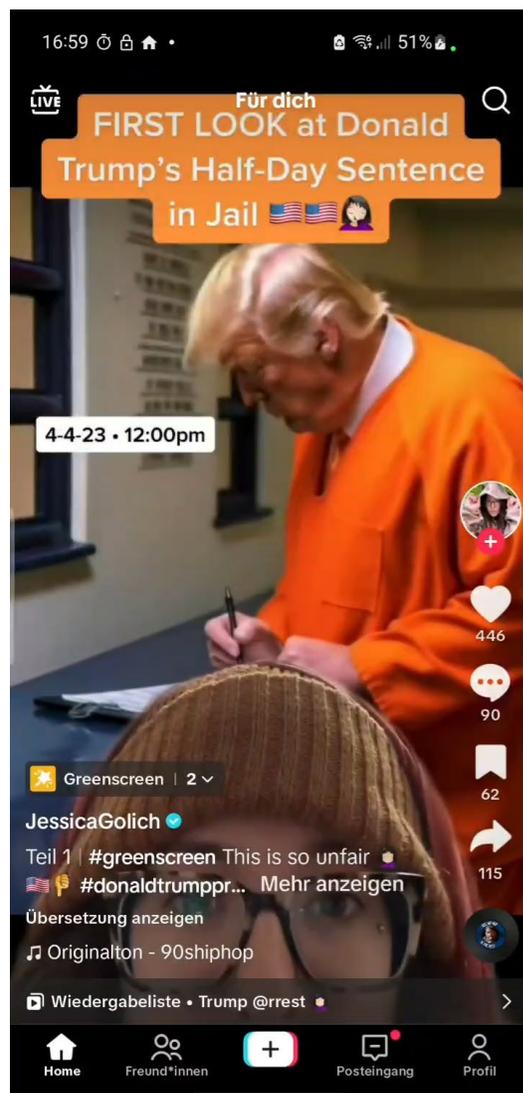


Akzeptanz



Teil III: Indikatorbasierte Interventionen

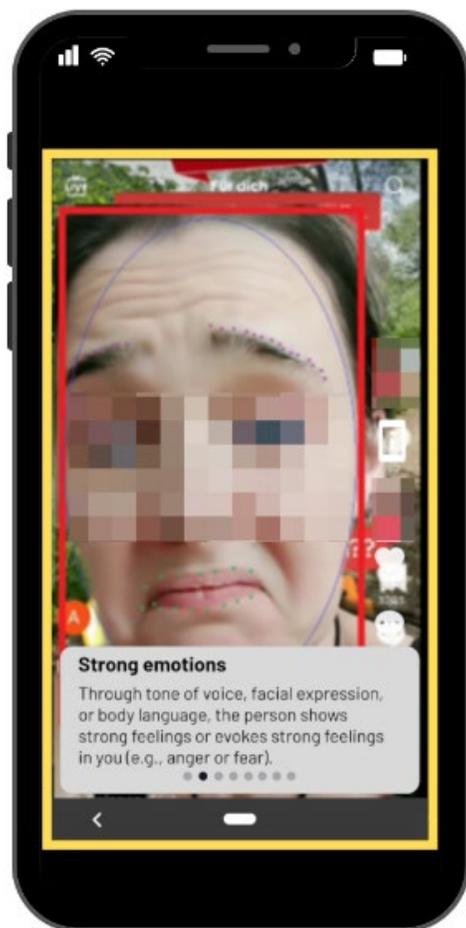
TikTok-Studie mit Jugendlichen: Stimuli



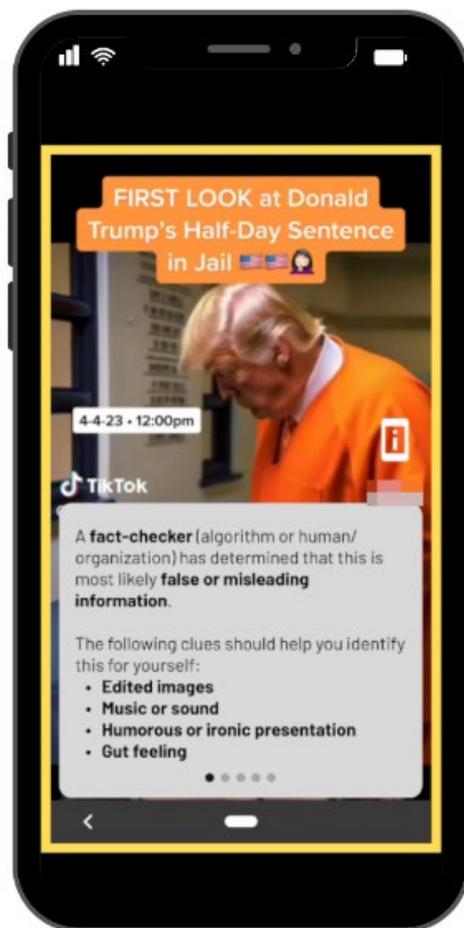
- Unterschiedlich erfolgreiche Erkennung von Misinformation ohne Hilfestellung
- Emotionalisierende Musik / Mimik / Sprache → wird **kaum als manipulierend** erkannt
- Bearbeitete Videos erkennen („Ein Finger zu viel“ etc.) → **Sehr gute Fähigkeiten**
- Video humorvoll oder ironisch → **Erfolgreiche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

Teil III: Indikatorbasierte Interventionen

TikTok-Studie mit Jugendlichen: Anzeige von Indikatoren



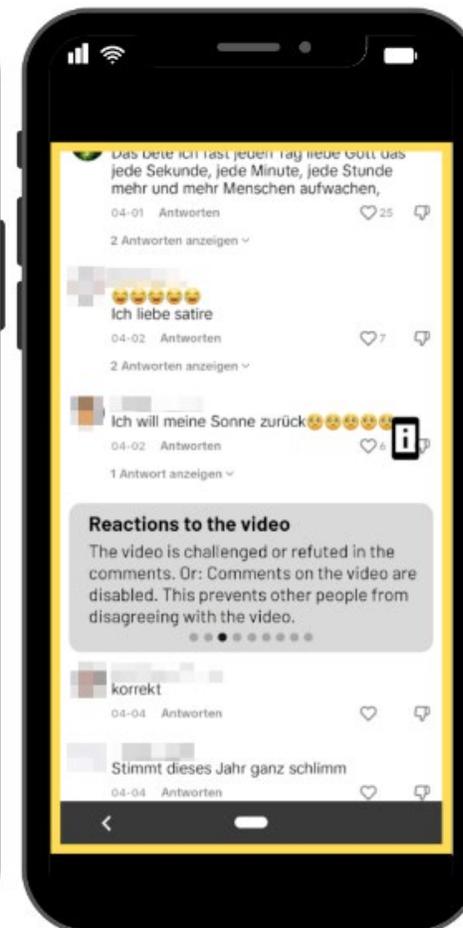
(a) Misinformation



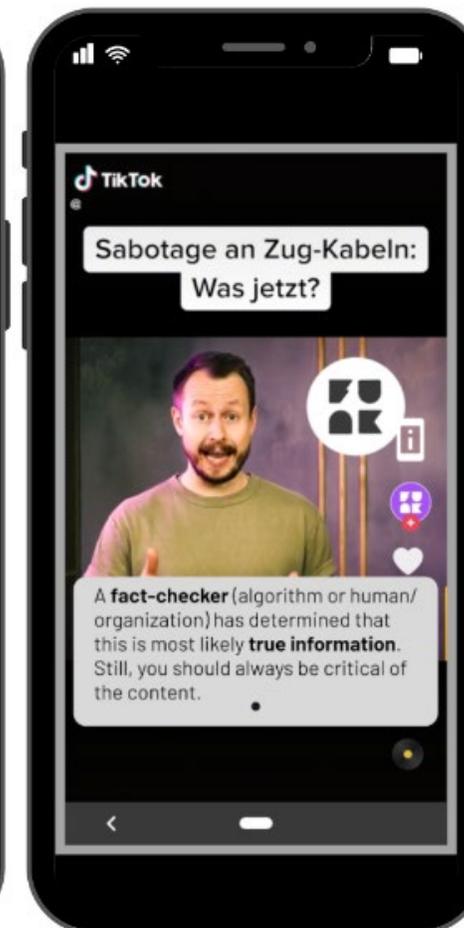
(b) Deep Fake



(c) Satire



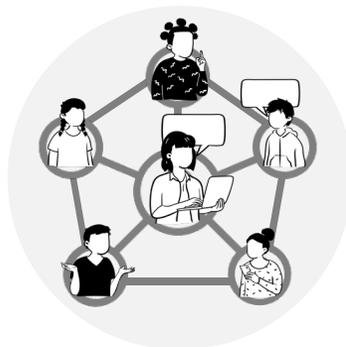
(d) Satire



(e) Wahre Nachrichten

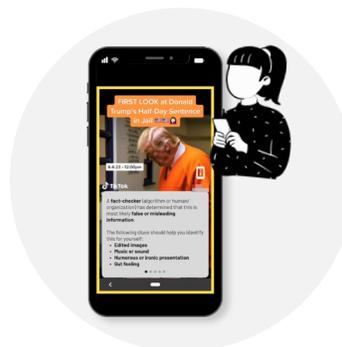
Teil III: Indikatorbasierte Interventionen

Status Quo



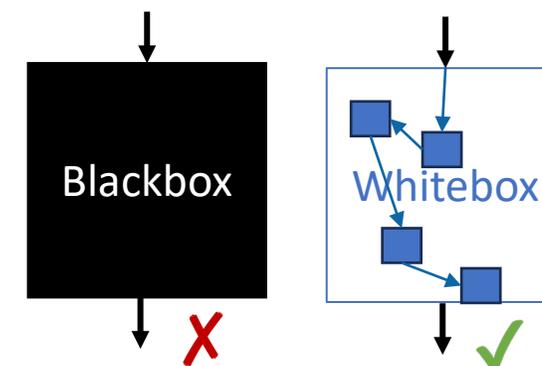
- Jugendliche nutzen **Merkmale von manipulierten Videos**
- Indikatoren auf verschiedenen Ebenen **erweitern und bestätigen** die Wahrnehmungen

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

① PEASEC | ② Information Warfare | ③ Cyberwar Warfare | ④ Ausblick

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

CYWARN
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)**

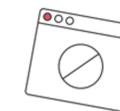
- Langjährige Studie mit **Länder-CERTs**
 - CERTs verbringen **täglich mehrere Stunden** mit **Monitoring** von Cybersecurity-Kommunikation
 - **Informationsüberfluss**

Mehr als **2.000** Schwachstellen in Softwareprodukten (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

“

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)



Cybersicherheits-Lagebild: Open Data Observatory

Open Data Observatory
admin

Data set: 8 selected
Show Posts of last: All time
Dashboard Refresh Time: 600s
Classifier: None
Filter Profile
Currently shown feeds: 4 of 6

Security Advisories

Sources:

Cisco Secure Network Analytics Remote Code Execution Vulnerability Priority: 8.2 CVSS Score: 9.1

Affected products: [Secure Network Analytics](#)

Source: [Cisco Security Advisory](#)

A vulnerability in the web-based management interface of Cisco Secure Network Analytics, formerly Cisco Stealthwatch Enterprise, could allow an authenticated, remote attacker to execute arbitrary commands as an administrator on the underlying operating system. This vulnerability is due to insufficient user input validation by the web-based management interface of the affected software. An attacker could exploit this vulnerability by injecting arbitrary commands in the web-based management interface. A successful exploit could allow the attacker to make configuration changes on the affected device or cause certain services to restart unexpectedly. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sta-sec-rce-2hyb9kfk> Attention: Simplifying the Cisco portfolio includes the renaming of security products under one brand: Cisco Secure. For more information, see Meet Cisco Secure. Security Impact Rating: Medium CVE: CVE-2022-20797

Show less

Cisco DNA Center Privilege Escalation Vulnerability Priority: 7.9 CVSS Score: 8.8

Affected products: [Dna Center](#)

Source: [Cisco Security Advisory](#)

A vulnerability in the management API of Cisco DNA Center could allow an authenticated, remote attacker to elevate privileges in the context of the web-based management interface on an affected device. This vulnerability is due to the unintended exposure of sensitive information. An attacker could exploit this vulnerability by inspecting the responses from the API. Under certain

Show more

Cisco Application Policy Infrastructure Controller and Cisco Cloud Network Controller Cross-Site Request Forgery Vulnerability Priority: 7.9 CVSS Score: 8.8

Affected products: [Cloud Network Controller](#) [Application Policy Infrastructure Controller](#)

Source: [Cisco Security Advisory](#)

A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based

Show more

Common Vulnerabilities and Exposures

Common Vulnerability Scoring System:

CVE-2022-26651 Priority: 8.0 CVSS Score: 9.8

Affected products: [Certified Asterisk](#) [Asterisk](#)

An issue was discovered in Asterisk through 19.x and Certified Asterisk through 16.8-cert13. The func_odbc module provides possibly inadequate escaping functionality for backslash characters in SQL queries, resulting in user-provided data creating a broken SQL query or possibly a SQL injection. This is fixed in 16.25.2, 18.11.2, and 19.3.2, and 16.8-cert14.

Published: 2022-04-15 07:15:00
Last modified: 2022-11-17 03:15:00

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	Partial
Base Score	7.5

References:

- <https://downloads.asterisk.org/pub/se...>
- <https://downloads.asterisk.org/pub/se...>
- [http://packetstormsecurity.com/files/...](http://packetstormsecurity.com/files/)
- <https://lists.debian.org/debian-its-a...>

Show less

CVE-2022-3955 Priority: 8.0 CVSS Score: 9.8

Affected products: [Crm42](#)

A vulnerability was found in tholum crm42. It has been rated as critical. This issue affects some unknown processing of the file crm42/class/class.user.php of the component Login. The manipulation of the argument user_name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-213461 was assigned to this vulnerability.

Show more

CVE-2022-3956 Priority: 8.0 CVSS Score: 9.8

Affected products: [Hims](#)

A vulnerability classified as critical has been found in trubeau UIUC 3.1. Affected is an unknown

Show more

Indicators of Compromise

Malwares:

win.lokipws http Confidence level is high (100%)

IoC: http

IoC Type: URL that is used for botnet Command&control (C&C)

Threat Type: Indicator that identifies a botnet command&control server (C&C)

First seen: 2022-11-28 15:10

Reporter: abuse_ch

Malware: win.lokipws

Show less

win.recordbreaker http Confidence level is high (100%)

IoC: http

IoC Type: URL that is used for botnet Command&control (C&C)

Threat Type: Indicator that identifies a botnet command&control server (C&C)

First seen: 2022-11-28 15:00

Reporter: abuse_ch

Malware: win.recordbreaker

Show less

win.ridder http Confidence level is high (100%)

IoC: http

IoC Type: URL that is used for botnet Command&control (C&C)

Threat Type: Indicator that identifies a botnet command&control server (C&C)

Show more

Social Media Posts

Data sources:

2022-11-28 15:35 by Bart R. McDonough

This new threat uses @GoogleAds and cracked #software. via @HackRead <https://t.co/xhaZVnIYW> #cybersecurity #cyberaware #security #IT #CyberSec #ransomware #malware #phishing #data #technology #cloud #cybersmart #managedIT #database #CTOs #CTO #cyberattack 1

2022-11-28 15:34 by m3oWuT

RT @sansforensics: NEW #DFIR POSTER | #MALWAREANALYSIS:TIPS & TRICKS by #FOR610 course author @lennyzeltser This poster provides a starting... 1

2022-11-28 15:34 by Oprea Andrei

@SuperDaltron I would want feedback to be in it, because it's Ben's favourite Alien. It's an important part of his character. Remember when Malware stole the Conductoid DNA from the Omnatrix and destroyed it? And then he was happy when he got it back? 1

2022-11-28 15:34 by @DyeAnna7

@DyeAnna7 @mbinya_1 alternatively you can just infect your w because her cctv, phone, TV, and homepod is connected to the it's an exploit in metasploit called "Memory-Resident Malware."

2022-11-28 15:33 by Bjdjdv Hsjsv

<https://t.co/6TVKJUeUz0> 1

2022-11-28 15:33 by Filipi Pires

Pyramid: Python scripts to evade EDRs <https://t.co/nGt0K44eg> #malware #cyber #pentesting #malwareanalysis #infosec #red #infosec #threat hunting #bugbounty #tools #offensivesecurity

2022-11-28 15:33 by Emiliano Carlesi

Threat on hxxps://7307[.]voto/ #malware #dynadot 1

2022-11-28 15:32

VCV-Chat

08:22 Jane Doe: Hallo zusammen, ich habe in den Medien von einer Sicherheitslücke bezüglich der SSL-Zertifikate in der Konferenzsoftware Cisco Webex erfahren. Hat jemand dazu weitere Informationen, die er mit uns teilen könnte? Vielen Dank.

Type something and hit enter to send...

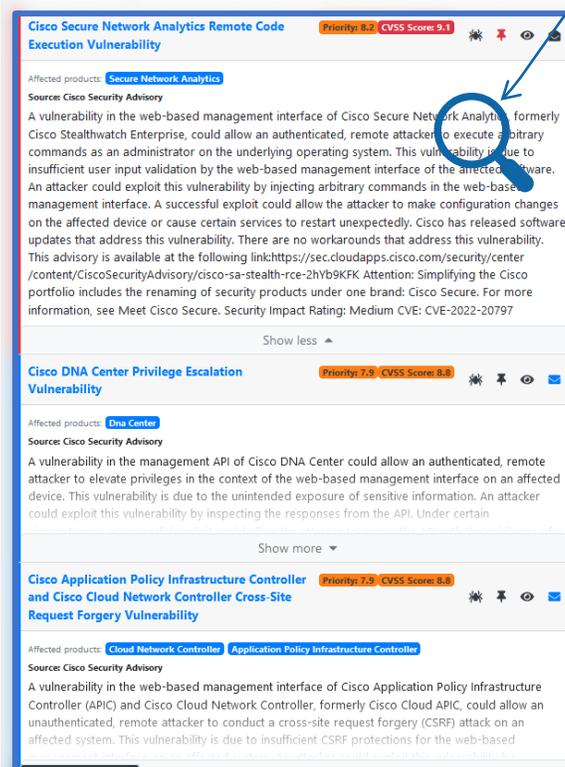
Send

Cybersicherheits-Lagebild: Open Data Observatory



KI zur Ermittlung der Relevanz

- Einbezug des CERT-Umfelds und der Kritikalität



Cisco Secure Network Analytics Remote Code Execution Vulnerability Priority: 8.2 CVSS Score 9.1

Affected products: **Secure Network Analytics**
Source: Cisco Security Advisory

A vulnerability in the web-based management interface of Cisco Secure Network Analytics, formerly Cisco Stealthwatch Enterprise, could allow an authenticated, remote attacker to execute arbitrary commands as an administrator on the underlying operating system. This vulnerability is due to insufficient user input validation by the web-based management interface of the affected software. An attacker could exploit this vulnerability by injecting arbitrary commands in the web-based management interface. A successful exploit could allow the attacker to make configuration changes on the affected device or cause certain services to restart unexpectedly. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealth-rce-2hyb9KFK> Attention: Simplifying the Cisco portfolio includes the renaming of security products under one brand: Cisco Secure. For more information, see Meet Cisco Secure. Security Impact Rating: Medium CVE: CVE-2022-20797

Show less

Cisco DNA Center Privilege Escalation Vulnerability Priority: 7.9 CVSS Score 8.8

Affected products: **Dna Center**
Source: Cisco Security Advisory

A vulnerability in the management API of Cisco DNA Center could allow an authenticated, remote attacker to elevate privileges in the context of the web-based management interface on an affected device. This vulnerability is due to the unintended exposure of sensitive information. An attacker could exploit this vulnerability by inspecting the responses from the API. Under certain

Show more

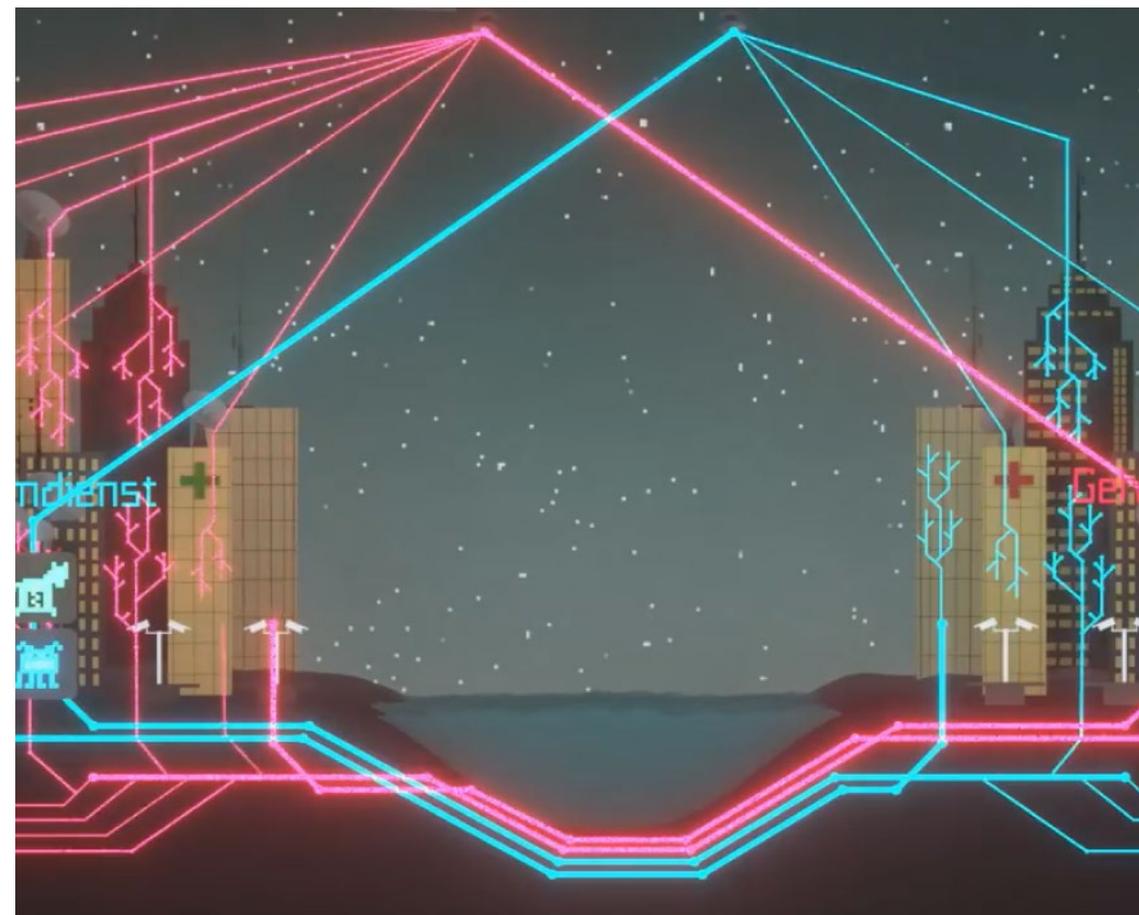
Cisco Application Policy Infrastructure Controller and Cisco Cloud Network Controller Cross-Site Request Forgery Vulnerability Priority: 7.9 CVSS Score 8.8

Affected products: **Cloud Network Controller Application Policy Infrastructure Controller**
Source: Cisco Security Advisory

A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based

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**



Abbau der Schwachstellenvorräte der Staaten



TECHNISCHE
UNIVERSITÄT
DARMSTADT

mit



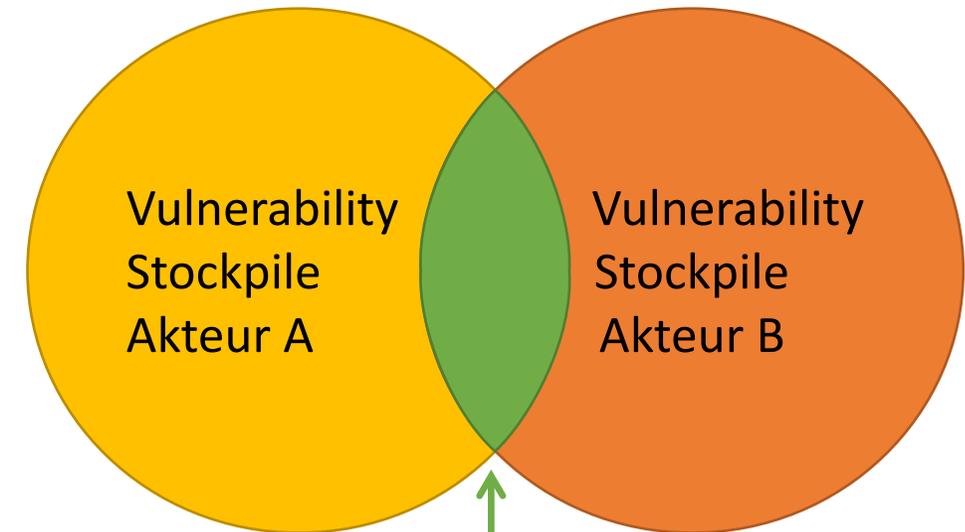
ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

■ 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



Menge an Vulnerabilities
für potentielles Disclosure

Technische Lösungen für Cyberabrüstung

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

mit



ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

- Basierend auf **interactive MultiParty Computation (MPC)**
 - n Akteure berechnen vereinbarte Funktion f auf ihren jeweiligen geheimen Eingaben x_1, \dots, x_N
 - Austausch des berechneten Ergebnis $f(x_1, \dots, x_N)$
- Abgleich der Ergebnisse $f(x_1, \dots, x_N)$ über Private Set Intersection (PSI) Algorithmus
- Akteur erhält Information darüber, ob/welche seiner Eingaben eine Kollision erzeugt haben

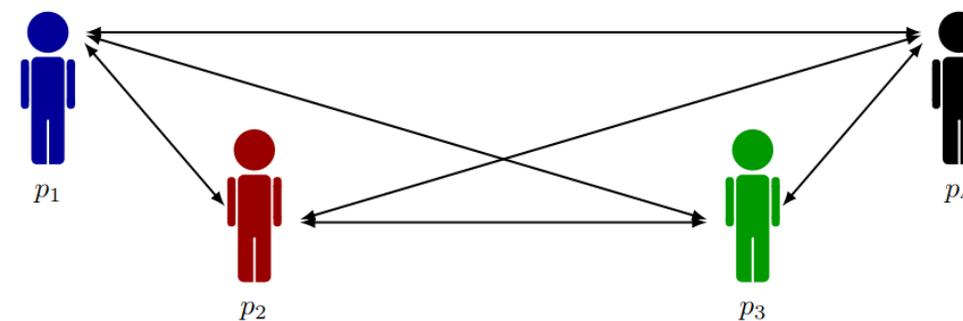


Fig. 2. MPC setting with four participating parties p_1, \dots, p_4 .



Technische Lösungen für Cyberabrüstung (ExTRUST)

Datenschutzfreundliches Depletion-System für zwischenstaatliche Beziehungen

mit



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 $n \approx 10$ bei einer Komplexität $O(N^2)$
- Abgleich erfordert Kooperation
- Technische Sicherheit vs. politisches Handeln von Staaten



① PEASEC | ② Information Warfare | ③ Cyber Warfare | ④ **Ausblick**

Ausblick

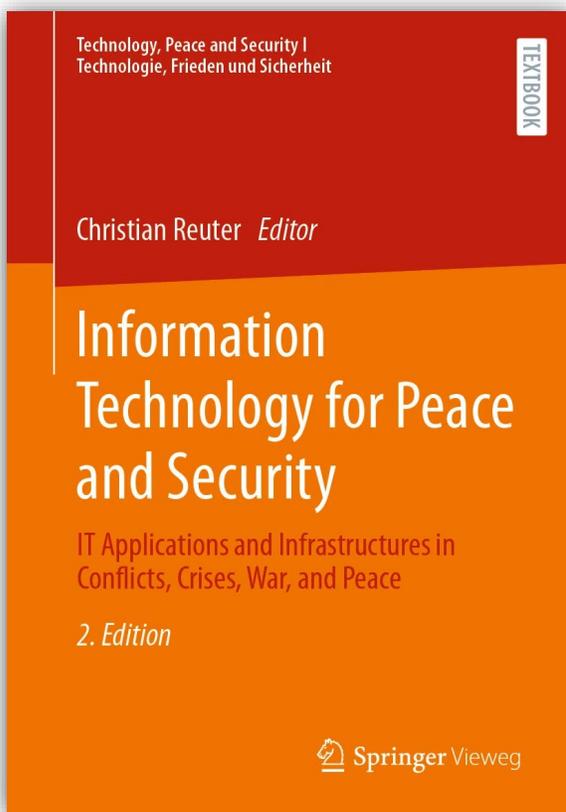
Prof. Dr. Dr. Christian Reuter

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)

... 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



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“



Hessisches
Ministerium des
Innern, für Sicherheit
und Heimatschutz



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>.