Wer sagt, was Phase ist

Analyse · Öffentlich

Über die Gefährlichkeit unbequemer Wahrheiten in einer Welt, in der digitale Identität zentral gespeichert und spurenlos kompromittiert werden kann.

Christer Häberli · philosophenstudio.de · 13. September 2026 Bezug: BWS I–V, BWS-EA-2026-09-13, BWS-SR-2026-09-13

I. Ein einfaches Prinzip

Es gibt ein einfaches Prinzip, das sich in menschlicher Kommunikation immer wieder beobachten lässt: Wenn jemand etwas sagt, das falsch ist, kann man sich entspannt zurücklehnen. Falsches erodiert. Schwarmintelligenz, die kollektive Prüfung von Aussagen durch viele unabhängige Beobachter, erledigt das zuverlässig, sachlich, ohne große Aufregung. Wer eine offensichtlich haltlose These aufstellt, wird ignoriert oder ruhig widerlegt.

Wenn jedoch jemand etwas sagt, das der Realität entspricht, und diese Realität für andere unbequem ist, geschieht etwas anderes. Es folgt massive Abwehr. Nicht gegen das Argument, sondern gegen die Person. Der Inhalt wird nicht geprüft; stattdessen wird der Überbringer angegriffen, degradiert, in die Ecke gedrängt.

> Wäre die Aussage falsch, könnte man sie ignorieren. Die Intensität der Abwehr ist selbst ein Befund über den Wahrheitsgehalt des Gesagten.

Das ist kein psychologischer Sonderfall. Es ist ein strukturelles Muster. Und es wiederholt sich auf jeder Skalierungsstufe, vom Einzelgespräch bis zur institutionellen Reaktion eines Staates.

II. Wenn Systeme dasselbe tun

Ein System, ob Unternehmen, Behörde oder politische Struktur, erbt die Abwehrmechanismen der Menschen, die es gebaut haben. Nur sind diese Mechanismen dann institutionalisiert. Sie werden mit Ressourcen ausgestattet: mit Rechtsabteilungen, PR-Strategien, bürokratischen Verfahren, medialer Reichweite.

Das Prinzip bleibt dasselbe. Wer innerhalb eines Systems auf einen realen Missstand hinweist, wird nicht als Problemlöser behandelt, sondern als Störenfried. Wer einen systemischen Fehler benennt, wird ausgegrenzt: nicht weil er falsch liegt, sondern weil er recht hat. Das System schützt nicht die Wahrheit. Es schützt seine Legitimation.

Ebene	Reaktion auf falsche Kritik	Reaktion auf zutreffende Kritik
Individuum	Schulterzucken, kurze Richtigstellung	Gegenangriff, Degradierung der Person
Gruppe	Sachliche Widerlegung durch Mehrheit	Ausgrenzung des Kritikers, Solidarisierung
Institution	Pressemitteilung, Vergessen	Rechtliche Verfolgung, Berufsruinierung, soziale Isolation
Staat	Keine Reaktion oder minimale Reaktion	Überwachung, Kriminalisierung, Spurenlosigkeit

Der Aufwand, der betrieben wird, um einen Kritiker mundtot zu machen, ist proportional zur Bedrohung, die er für das System darstellt. Und eine Bedrohung stellt er nur dar, wenn er recht hat.

III. Die technische Dimension: was heute möglich ist

Bisher war der Preis für unbequeme Wahrheiten sozial, beruflich, juristisch. Man verlor Freunde, Aufträge, Reputation. Das ist gravierend. Aber es hatte Grenzen. Der Körper war sicher. Die Wohnung war sicher. Das Gespräch unter vier Augen war sicher.

Diese Grenzen existieren technisch nicht mehr.

Pegasus ist eine kommerzielle Überwachungssoftware, die von staatlichen Stellen weltweit eingesetzt wird. Sie infiziert Smartphones ohne jede Nutzerinteraktion; keine Handlung, kein Klick, kein Fehler des Betroffenen ist erforderlich. Nach der Infektion besteht vollständiger Zugriff: Mikrofon, Kamera, alle Nachrichten, alle Passwörter, Standort in Echtzeit. Die Infektion ist für den Betroffenen nicht erkennbar. Die Spyware löscht sich selbst bei Entdeckungsrisiko.

Der EU-Untersuchungsausschuss PEGA hat in seinem Abschlussbericht (Mai 2023) forensisch bestätigt: Pegasus wurde in EU-Mitgliedstaaten (Spanien, Ungarn, Polen, Griechenland) von staatlichen Stellen gegen eigene Staatsbürger eingesetzt. Gegen Journalisten. Gegen Anwälte. Gegen Oppositionspolitiker. Menschen, die sagten, was Phase war.

Dokumentierter Befund: PEGA Final Report, Mai 2023: "The use of Pegasus and equivalent surveillance spyware in the European Union has been confirmed in several Member States, targeting journalists, lawyers, politicians, and civil society activists."

IV. Die neue Struktur: Pflichtbürgerkonto und digitale Identität

Parallel dazu entsteht eine neue Infrastruktur. Der Koalitionsvertrag von CDU/CSU/SPD (2025) legt fest: "Jeder Bürger und jede Bürgerin erhält verpflichtend ein Bürgerkonto und eine digitale Identität."

Das geplante System (BundID, DeutschlandID, EUDI-Wallet) zentralisiert an einem einzigen digitalen Punkt, was früher auf viele unabhängige Stellen verteilt war:

- Alle Verwaltungskommunikation (Anträge, Bescheide, Behördenkontakt)
- Identitätsnachweis (Ausweis-Funktion)
- Digitale Signaturen (Rechtsgültigkeit)
- Dokumentenspeicherung
- Zahlungsvorgänge (nach vollständiger Implementierung)

Alles davon läuft auf einem einzigen Endgerät. Demselben Endgerät, das Pegasus kompromittiert.

V. Was das bedeutet: wenn jemand will, jemanden zu zerlegen

Die Möglichkeit, eine Person vollständig zu kompromittieren, existiert. Sie ist keine Theorie. Sie wurde dokumentiert. Was neu ist, ist die Tiefe dessen, was künftig kompromittierbar ist.

Bisher: Kommunikation, Standort, Kontakte. Künftig, mit einem zentralen Pflichtbürgerkonto: Kommunikation, Standort, Kontakte; und zusätzlich die gesamte staatsbürgerliche Existenz der Person.

Wer Zugriff auf das Endgerät hat, hat Zugriff auf das Bürgerkonto. Wer Zugriff auf das Bürgerkonto hat, kann Anträge stellen, Bescheide empfangen, Identitätsnachweise verwenden, Signaturen erzeugen, im Namen des Opfers. Unsichtbar. Spurenlos.

Konkrete Möglichkeiten bei kompromittiertem Gerät und Bürgerkonto:

- Vollständige Überwachung aller Behördenkommunikation in Echtzeit
- Impersonation: Anträge und Signaturen im Namen der Zielperson
- Extraktion aller hinterlegten Identitätsdaten und Dokumente
- Manipulation von Zahlungsvorgängen (nach vollständiger Wallet-Implementierung)
- Aufbau eines vollständigen staatsbürgerlichen Profils der Zielperson

Für die betroffene Person ist das nicht erkennbar. Kein Alarm. Kein Hinweis. Kein Symptom. Die Person lebt weiter in dem Glauben, ihre digitale Identität sei intakt.

VI. Die Konvergenz: warum sie relevant ist

Drei Entwicklungslinien konvergieren:

Erste Linie: Wer sagt, was Phase ist, zahlt einen Preis. Das ist historisch konstant und psychologisch gut erklärbar. Die Intensität der Abwehr korreliert mit dem Wahrheitsgehalt der Aussage, nicht mit ihrer Falschheit.

Zweite Linie: Spyware der Pegasus-Klasse ermöglicht die vollständige, spurenlose Kompromittierung von Endgeräten. Sie wurde nachweislich gegen Menschen eingesetzt, die sagten, was Phase war.

Dritte Linie: Ein Pflichtbürgerkonto für 84 Millionen Menschen zentralisiert die gesamte staatsbürgerliche digitale Existenz auf genau dem Endgerät, das Pegasus kompromittiert.

> Das Werkzeug existiert. Die Infrastruktur wird gebaut. Der Anreiz, jemanden zum Schweigen zu bringen, der sagt, was Phase ist, ist so alt wie die Sprache selbst.

Die Konvergenz dieser drei Linien ist keine Spekulation. Sie ist die logische Folge dokumentierter Tatsachen.

VII. Die Schwarmintelligenz als letzter Schutz: ihre Grenzen

In offenen, funktionierenden Informationsumgebungen ist Schwarmintelligenz ein verlässlicher Korrektiv-Mechanismus. Falsches wird geprüft, zerlegt, vergessen. Richtiges setzt sich durch, manchmal langsam, aber es setzt sich durch.

Dieser Mechanismus hat eine Voraussetzung: Die Person, die sagt, was Phase ist, muss noch sprechen können. Sie muss erreichbar sein. Ihre Glaubwürdigkeit darf nicht systematisch zerstört worden sein. Ihre digitale Identität muss noch die ihre sein.

Wenn ein hinreichend ausgestatteter Akteur diese Voraussetzungen aufhebt, durch Kompromittierung des Endgeräts, durch Impersonation, durch vollständige Überwachung, durch gezielte Nutzung der zentralisierten Identitätsinfrastruktur, dann greift der Korrektiv-Mechanismus nicht mehr. Nicht weil die Aussage falsch war. Sondern weil die Person, die sie gemacht hat, effektiv nicht mehr existiert.

VIII. Fazit

Es gab immer Menschen, die sagten, was Phase war. Es gab immer Strukturen, die das zu verhindern versuchten. Das Muster ist nicht neu.

Was neu ist, ist das Ausmaß der verfügbaren Mittel. Und was neu ist, ist die Infrastruktur, die gerade, für alle verpflichtend, gebaut wird.

Die Möglichkeit, eine Person vollständig digital zu zerlegen, ihre Identität, ihre Kommunikation, ihre staatsbürgerliche Existenz, ist keine zukünftige Gefahr. Sie ist eine gegenwärtige Realität, für die gerade die technische Grundlage flächendeckend gelegt wird.

Wir wissen das, weil es dokumentiert ist. Weil Ausschüsse es festgestellt haben. Weil Forensiker es nachgewiesen haben. Weil Menschen davon betroffen waren, die sagten, was Phase war.

Schlussfolgerung: Wer in einer Welt mit zentralisierter digitaler Identität und nachgewiesenen Werkzeugen zur spurenlosen Endgeräte-Kompromittierung sagt, was Phase ist, trägt ein strukturelles Risiko, das frühere Generationen nicht kannten. Die Möglichkeit, jemanden vollständig zu zerlegen, besteht. Sie wird genutzt werden, wie sie bereits genutzt wurde. Das ist keine Prognose. Das ist eine Ableitung aus dem, was wir bereits wissen.

Quellenhinweise

Quelle	Typ
Koalitionsvertrag CDU/CSU/SPD 2025, Kapitel Digitalisierung	Politisches Dokument

Quelle	Typ
OZG Paragraph 3, Bundesgesetz (aktuell)	Gesetzestext
EU-Untersuchungsausschuss PEGA, Abschlussbericht Mai 2023	Parlamentarischer Bericht
Citizen Lab, University of Toronto, Pegasus Technical Analysis (2021)	Forensischer Bericht
Amnesty International Tech, Forensic Methodology Report (2021)	Forensischer Bericht
Forbidden Stories / Pegasus Project (2021), Investigativkonsortium	Investigativrecherche
Citizen Lab, Catalangate (2022)	Forensischer Bericht
BWS-SR-2026-09-13, Strukturrisiko Digitale Zwangsidentität	Eigenanalyse

---

Christer Häberli · philosophenstudio.de · 13. September 2026 · Öffentlich