2039 Resilienz durch dezentrale Vernetzung (November 2026)



"Trusted WEB 4.0 is the Integration of all resources available via the Web into an overall system.

Machines, devices and people are globally accessible, organized in decentralized, anonymous structures.

Trusted WEB 4.0 maps pre-digital social structures.

The value chains are being reorganised.“
(Olaf Berberich, 2007)

2039 – Resilienz durch dezentrale Vernetzung

Freie Hintergrundstudie zur Jahresreihe 1985–2045

Der 13. Oktober 2026: Der Moment, in dem die Abhängigkeit sichtbar wurde

In der Nacht vom 13. auf den 14. Oktober 2026 wurden militärische Starshield-Terminals in der Ukraine gedrosselt – jene Terminale, die Drohnen steuern, Raketen abfangen und die Führungskommunikation tragen. Nicht Russland legte sie lahm, sondern der wichtigste Verbündete; SpaceX drosselte die Bandbreite der beweglichen Terminals und setzte ein Tempo-Limit von 161 km/h durch. [1] Die EU-Außenbeauftragte musste einräumen, dass Europa kurzfristig keine Alternative besitzt, und Europas eigenes Satellitennetz IRIS² startet frühestens 2029, voll operativ ein Jahr später. [2] Diese Nacht ist der Ausgangspunkt dieser Studie, denn sie zeigt in einer einzigen Beobachtung, worum es 2039 gehen muss: Eine Gesellschaft, deren Kommunikation, Navigation und Warnung an wenige zentrale Schichten gekoppelt ist, verfügt im entscheidenden Moment nicht über ihre eigenen Systeme. Sie verfügt über eine Erlaubnis.

Eine störungsanfällige Gegenwart – die Beleglage bis 2026

Die Sorge ist keine theoretische. Russland kann GPS-Signale vom Kaliningrad aus über Hunderte Kilometer fälschen; die Zahl der bekannten Störsender ist von drei auf 36 Antennen gestiegen. [3] Am 24. August 2026 liefen in Polen Telefone, Drohnen und Schiffe „blind“. [4] Der Forschungsdienst des US-Kongresses führt Navigationsstörung offiziell als Instrument russischer hybrider Kriegsführung. [5] In der Ostsee wurden der Balticconnector und ein Datenkabel 2023 beschädigt, das Seekabel C-Lion1 zwischen Finnland und Deutschland 2024 – der deutsche Verteidigungsminister sprach von „Sabotage“. [6,7] Auf der digitalen Seite zeigten zwei Ereignisse dasselbe Muster: Die globale CrowdStrike-Störung vom Juli 2024 legte Flugzeuge auf den Boden und ließ Kliniken nicht operieren; [8] die IT-Störung der Charité legte Aufnahme, Behandlung und Dokumentation still. [9] Die Vereinten Nationen warnen vor einer „digitalen Pandemie“ – einer globalen Kettenreaktion, in der ein einzelner Fehler ganze Versorgungsketten mitreißt. [10] Die Gemeinsamkeit aller Fälle ist nicht die Ursache, sondern die Struktur: Immer war eine zentrale Instanz der einzelne Punkt, an dem eine ganze Gesellschaft ausgeschaltet werden konnte. Zentrale IT ist im Cyberkrieg das ideale Ziel – ein Ziel, das der Gegner nicht einmal selbst treffen muss, wie CrowdStrike bewies.

2039: Zentrale IT wird verboten

Vor diesem Hintergrund gilt 2039 eine klare Regel: **Innerhalb des EU-D-S ist zentrale IT für kritische Infrastruktur verboten.** Das Verbot richtet sich nicht an Staaten – das EU-D-S ist ein Parallelsystem neben der bestehenden Ordnung,

und nach dem Stand von 2038 ist rund die Hälfte der Bevölkerung in ihm organisiert; die andere Hälfte lebt und arbeitet unverändert im bestehenden System. Diese Spaltung ist kein Mangel des Konzepts, sondern Teil seiner Wirkung: 2038 zeigt, dass die Spaltung sogar einen Krieg verhindert, solange die Autokraten noch eine Chance sehen, sich durchzusetzen. Wer sich noch durchsetzen kann, bleibt innerhalb der Ordnung, die er ablehnt.
Das Verbot gilt für die Bereiche, die im EU-D-S organisiert sind – Krankenhäuser, Verwaltungen, Warnung und Zahlungsverkehr der Teilnehmer und Regionalcluster. Es ist der Endpunkt einer Lernkurve, die 2024 begann: Eine Gesellschaft, die ihre kritischen Systeme an wenigen zentralen Stellen bündelt, bietet jedem Angreifer ein einziges, unschwer zu findendes Ziel. **Resilienz entsteht nicht durch Abschottung, sondern durch Redundanz in die Breite.** Nicht die Isolation vom Netz macht widerstandsfähig, sondern die Verteilung der Netzfähigkeit auf Tausende lokale Punkte, von denen jeder den Ausfall der anderen auffangen kann.

Netze und Konnektivität: Der Hebel liegt im Datenvolumen

Die erste Gruppe zentraler Abhängigkeiten betrifft die physischen und logischen Netze: Satelliten-Internet, Satellitennavigation, Seekabel, Mobilfunkvermittlungsstellen, DNS-Root-Server und zentrale Identitätsverwaltung. Hier gilt die entscheidende Eigenschaft des EU-D-S: Es speichert nur Metadaten und verzichtet auf den permanenten Aufbau zentraler Datenberge. Ein System, das die Hälfte der sonst üblichen Rechen- und Übertragungsleistung braucht, ist nicht unabhängiger von jedem Kabel – aber es bleibt funktionsfähig, wenn Kabel, Satelliten oder Vermittlungsstellen ausfallen. Die Truststation wird zum lokalen Netzknoten, der Gruppen offline versorgt; WLAN-Mesh-Strukturen und Drohnen als Relaisstationen (Anschluss an das Drohnenkonzept von 2038) überbrücken lokale Lücken. Identität und Verschlüsselung beruhen auf Truststation-Schlüsselsätzen und WAN-Anonymität statt auf zentralen Zertifikats- und Identitätsmonopolen; der PDS-Hardware-Standard schließt Hintertüren aus.
Dazu gehört eine analoge Ebene, die in der Digitaldebatte gern vergessen wird: der Amateurfunk. Er ist unabhängig von terrestrischer Infrastruktur, über die Gemeinschaft verteilt und ohne die „Choke Points“, an denen Mobilfunknetze zusammenbrechen; das Gerät läuft an der Autobatterie. [11] Beim Hurrikan Ida 2021 waren Funkamateure in ganzen Landstrichen der einzige funktionierende Meldeweg. [12] Im EU-D-S sind die Funkamateure anerkannte Spezialisten der Regionalcluster – Teil des Spezialisten-Regelwerks, nicht Hobby am Rand.

Vertiefung am Beispiel Starlink: Was dezentrale Maßnahmen wirklich ersetzen

Die Drosselung vom Oktober 2026 trifft die Ukraine nicht abstrakt. Betroffen sind vor allem die Abfangdrohnen, die russische Jet-Drohnen abfangen sollen – zu langsam mit Tempo-Limit; erst nach Tagen wurde es aufgehoben. [13] Europas erste Reflexion lautet: ein eigener Satellit. Aber IRIS² startet frühestens 2029 und

ist erst ein Jahr später voll operativ; die EU-Außenbeauftragte räumte ein, dass Europa diese Fähigkeit kurzfristig nicht ersetzen kann. [2] Die Ukraine hat deshalb einen zweiten Weg vorgelegt, der im Westen kaum beachtet wird: Nicht das Satellitennetz wird ersetzt, sondern das Bedürfnis nach der Verbindung im entscheidenden Moment. Fünf Maßnahmen sind belegt.

Glasfaser statt Funk. Ukrainische FPV-Drohnen fliegen mit Spulen von Glasfaserkabeln von zehn bis über zwanzig Kilometern Länge; die Steuerung läuft über das Kabel, nicht über Funk oder Satellit. Eine solche Drohne kann weder gestört noch abgeschaltet werden, weil es keine Verbindung gibt, die ein Dritter kontrolliert. [14] Beim staatlichen Beschleuniger-Programm Brave1 testeten über fünfzehn Hersteller Glasfaser-FPVs auf einer 20-Kilometer-Route – die Antwort auf die Frage „Was, wenn uns das Netz abgestellt wird?“ lautet hier: Es gibt kein Netz. [15]

Intelligenz am Rand. Das ukrainische Verteidigungsministerium meldete im August 2026 mehr als siebzig KI- und Maschinensicht-Systeme an der Front; erklärtes Ziel ist ein Rechner für Maschinensicht in jeder Frontdrohne. [16] Module wie das TFL-1 übernehmen die letzten 400 bis 500 Meter autonom, nach Zielfreigabe durch den Menschen – gebaut für den Endanflug mitten im Störfeld, für rund 100 US-Dollar; ein 18-Dollar-Chip reicht für die Zielbindung. [17,18] Wer die letzte Meile lokal löst, braucht im entscheidenden Moment keine Verbindung mehr – auch nicht in dem tiefen Luftraum, in dem elektromagnetische Störung die Satellitennavigation zusammenbrechen lässt. [19]

Sensoren in der Breite. Das ukrainische Start-up Zvook betreibt tausende akustische Sensoren über das Land verteilt; jeder Sensor kostet etwa 500 US-Dollar und erkennt Drohnen auf fünf, Marschflugkörper auf sieben Kilometern – nicht mit Radar, sondern mit einem auf Drohnengeräusche trainierten Erkennungsmodell. Beobachter vergleichen das System mit einem riesigen, dezentralen passiven Sonar. [20,21] Erstmals wurde die mobile Version auf der NATO-Übung BATT26 in Lettland erprobt. [22] Improvisationen desselben Typs – etwa auf Stangen montierte Handys als Luftlagensensoren – zeigen, wohin die Reise geht: weg vom einen, teuren, angreifbaren Sensor, hin zu vielen billigen. [23]

Bürger als Sensoren. Die App ePPO macht seit 2022 aus jedem Bürger einen Meldungsknoten: Wer eine Drohne sieht, richtet das Smartphone auf sie und drückt einen roten Knopf; die Flugabwehr erhält die Zielangabe. [24,25] Die Warnung überlebt jeden Zentralausfall, weil sie in der Bevölkerung lebt.

Navigation vom Boden. Das System Pokrova überlagert die Satellitennavigation landweit mit falschen Signalen vom Boden: Angreifende Shahed-Drohnen werden in leere Felder gelenkt. Im November 2024 wurden 95 von 188 angreifenden Drohnen auf diese Weise umgeleitet – ohne einen einzigen Satelliten. [26,27]

In ziviler Übersetzung sind das genau die Designprinzipien des EU-D-S: das lokale physische Medium (die Truststation als Netzknoten), die Intelligenz vor Ort statt in der zentralen Cloud (Verarbeitung am Gerät, Metadaten-Prinzip), Sensoren in der Breite statt eines zentralen Radars, die Bevölkerung als Teil der Warnkette (WAN-anonyme Meldungen, Regionalcluster-Eskalation, Drohnenbeauftragte je Häuserblock) und die bodenbasierte Navigation statt Satellitenabhängigkeit. **Der**

Ausweg aus der Starlink-Abhängigkeit führt nicht nur über eigene Satelliten – er führt über Systeme, die im entscheidenden Moment keine Verbindung brauchen.
Die Ehrlichkeitsregel gilt auch hier: Glasfaserdrohnen haben Reichweite- und Kabelgrenzen, die Terminal-KI trägt nur die letzten Meter, während der Anflug weiter netzabhängig bleibt; Zvook erkennt, bekämpft aber nicht; Pokrova ist selbst landweit-zentral organisiert. Den reichweitenstarken Satelliten ersetzt nichts davon vollständig. Die dezentralen Maßnahmen ersetzen nicht den Satelliten – sie verkleinern das, wofür der Satellit gebraucht wird. Und genau dieses Verkleinern ist die Resilienz.

Zentrale IT und Daten: Der Zentralmodus wird zum Ausnahmezustand

Die zweite Gruppe betrifft das, was 2024 und 2026 lahmlegte: zentrale IT in Krankenhäusern, Verwaltungen und Konzernen, zentrale Gesundheitsdaten, zentrale Verwaltungsportale. Die Antwort des EU-D-S sind dezentrale Systeme mit Admin-Kopien und Zentralmodus, wie sie die Patentanmeldung DE102016002956A1 beschreibt: Die unidirektionale Verbindung verhindert, dass ein Angriff von außen in die lokalen Systeme wandert; Admin-Kopien erlauben Wiederanlauf ohne zentrale Infrastruktur; der Zentralmodus existiert weiterhin – aber als bewusst erklärter Ausnahmezustand, nicht als Normalzustand. Gesundheitsdaten bleiben in der Hoheit der Patienten und werden vor Ort verarbeitet (die Linie, die 2040 zur Teilhabe im Alter führt). Verwaltungen organisieren sich nicht als Behördeninseln, sondern als Verwaltungscluster in der Genossenschaftslogik des EU-D-S.

Die Cloud-These: Wenn Zentralisierung zur Moral erklärt wird

Der Streit um die richtige Architektur hat 2026 eine bemerkenswerte Wendung genommen. Sam Altman erklärte, es sei aus globaler Allokationsperspektive „ziemlich schrecklich“, wenn Menschen eigene Modelle auf eigenen Computern rechnen ließen: Der weltweit begrenzte DRAM-Vorrat solle nicht in Privat-PCs liegen, sondern in Rechenzentren – „maximale Auslastung in der Cloud“ sei das Ziel. [28] Der Fehler liegt nicht in der Knappheit, sondern in der Folgerung: Aus einem Versorgungsproblem wird eine Moralfrage. Wer lokal rechnet, gilt als unsozial – und aus Abhängigkeit wird eine Tugend.
Das EU-D-S nimmt Altmans eigenes Kriterium ernst: Auslastung. Nur wird sie nicht durch die Cloud erreicht, sondern durch zwei dezentrale Prinzipien. Erstens: bedarfsgerechte Hardware statt Überkapazität. Truststationen und PDS-Geräte sind auf die Aufgabe dimensioniert, die sie tatsächlich haben – getmySense-Bewertungen, Validierung, Metadaten. Das Metadaten-Prinzip spart rund die Hälfte der Rechenleistung; wer keine Datenberge durch die Landschaft schiebt, braucht keine GPU-Farmen. Zweitens: Auslastung durch Aufgaben, nicht durch Ort. Der Roboter-Chip aus der 2037-Studie ist das Gegenbeispiel zur

Cloud-These. Er ist nicht deshalb ausgelastet, weil ein Hyperscaler ihn in eine Halle gestellt hat, sondern weil er im Intranet des Häuserblocks Koordinierungsaufgaben übernimmt: die Energieregelung nach den eigenen Patentanmeldungen, Wach- und Butler-Dienste, die Anwesenheitskoordination der Nachbarschaftskette, die Hilfevermittlung an die Truststation. Nachts, wenn der Butler ruht, rechnet derselbe Chip für den Block. **Auslastung entsteht nicht dadurch, dass die Hardware an einem Ort gebündelt wird – sondern dadurch, dass die Aufgaben in einer Nachbarschaft gebündelt werden.**

Die Zeit: die aufgelöste Abhängigkeit

Verborgener als die Navigation ist eine zweite Abhängigkeit des Satellitenzeitalters: die Zeit. GNSS ist der Weltzeitgeber geworden – Stromnetze synchronisieren sich über die GPS-Zeit, jede elektronische Transaktion trägt ihren Zeitstempel, und selbst das Versenden einer Nachricht hängt an einer gemeinsamen Uhr. Die Fachwelt warnt inzwischen, dass diese Zeitverteilung zu den verwundbarsten Infrastrukturen überhaupt gehört. [29,30] Der naheliegende Reflex der Resilienz-Debatte lautet: die verlorene Abhängigkeit lokal nachbauen – Zeitserver in jede Truststation, quarzgesteuerte Ersatzuhren, eine zweitebeste Version der Satellitenzeit.
Das Projekt „das EI“ [31] hat den Beweis erbracht, dass es auch ohne geht. Alle seine Entwicklungen sind ohne Zeitangabe programmiert. Das System misst die Helligkeit und weiß, ob Tag oder Nacht ist; es zeichnet Bewegung auf und erkennt das Geschehen aus der Abfolge; es sieht am PV-Ertrag, was die Sonne gerade tut. Nicht die Uhr entscheidet, sondern der Zustand der Umgebung – und der Zustand ist nicht abschaltbar. Erst wenn die absolute Zeit aus einem Systementwurf verschwindet, zeigt sich, dass sie nie die Voraussetzung war, sondern eine Gewohnheit. Deshalb beginnt diese Studie nicht bei der Technik, sondern bei der Denkweise: **Die zweitbeste Lösung ist die zuverlässige Nachbildung der verlorenen Abhängigkeit. Die beste Lösung ist, die Abhängigkeit nicht zu brauchen.**

Notfall, Warnung und Spezialisten: Erreichbarkeit statt Zentrale

Die dritte Gruppe betrifft die, die im Ernstfall zuerst gebraucht werden. Zentrale Warnsysteme haben sich als anfällig erwiesen: Cell Broadcast hängt an zentralen Vermittlungsstellen, Sirenen wurden über Jahrzehnte abgebaut. Das dezentrale europäische Katastrophenschutzsystem dreht die Logik um: Truststation-Nummern und Nachbarschaftsketten machen jeden Bürger erreichbar, Regionalcluster eskalieren Hilfeanfragen weiter, wenn die eigene Umgebung nicht antwortet. Notruf und Leitstellen werden durch dezentrale Hilfeanfragen ergänzt, die bei Überlastung oder Ausfall der zentralen Stelle ihren Weg trotzdem finden. Notfalllogistik und Grundversorgung halten Regionalcluster und Nachbarschaftshilfen vor, wo zentrale Verteilung ausfällt.
Die Spezialisten verdienen besondere Aufmerksamkeit, denn hier zeigt sich, dass

dezentrale Vernetzung keine Vereinsamung ist. Wissen darf nicht an wenigen Zentren hängen – aber es darf auch nicht in tausend isolierten Gruppen verschwinden. Spezialisten bleiben übergreifend vernetzt; ein klares Regelwerk definiert, wann eine dezentrale Gruppe Hilfe von außen anfordert. Das Regelwerk ersetzt die zentrale Disposition: Nicht die Leitstelle entscheidet über Hilfe, sondern eine definierte, trainierte Anforderung. getmySense-validiertes Wissen wird verteilt statt in Expertenmonopolen gebündelt, und lokale Befähigung – bis hin zum Drohnenbeauftragten je Häuserblock – senkt die Zahl der Fälle, in denen überhaupt ein Spezialist von außen gebraucht wird.

Wenn der Gegner die Warnung selbst hackt

Die Beleglage 2026 zwingt zu einem eigenen Punkt: Warnkanäle sind nicht nur störanfällig, sie sind angreifbar. Im selben Jahr wurden die offiziellen Notfall-Apps der Ukraine und Russlands gehackt – Bürger erhielten gefälschte Strahlen- und Kriegsalarme. [32] In Rumänien kursierten gefälschte RO-ALERT-Warnungen, mit dem ausdrücklichen Ziel, Panik zu erzeugen. [33] Bei den Waldbränden in British Columbia verbreiteten sich gefälschte Evakuierungsbefehle in Behördenoptik. [34] Ein gehackter Zentralkanal ist gefährlicher als ein ausgefallener: Er zerstört die Vertrauensbasis, auf der jede Warnung ruht. Die Antwort des EU-D-S ist doppelte Absicherung: Warnungen gelten nur signiert von der lokalen Truststation, deren Echtheit der Empfänger selbst prüfen kann – und jede Warnung läuft durch die Validierung von getmySense und den Finder-Fake-Schalter, bevor sie eine Nachbarschaftskette auslöst. Ein gefälschter Zentralalarm erreicht die Breite nicht, weil die Breite nicht auf ihn hört, sondern auf ihre Knoten.

Die Quanten-Migration: Wer die Schlüssel hält

Die 2030er sind das Jahrzehnt einer erzwungenen Neuverteilung: Die Kryptographie des letzten Jahrzehnts wird unverzüglich abgelöst, weil Angreifer verschlüsseltes Material bereits heute sammeln, um es später mit Quantenrechnern zu entziffern – „harvest now, decrypt later“. [35] Die USA setzten per Anordnung vom Juni 2026 harte Fristen: kritische Systeme auf Post-Quanten-Verfahren bis Ende 2030, digitale Signaturen bis Ende 2031. [36] Das BSI setzte vergleichbare Enddaten, die nationale Umsetzungsrichtlinie folgte am 12. Oktober 2026. [37,38] Diese Migration erzwingt ohnehin neue Schlüssel für alles – und genau darin liegt die eigentliche Frage von 2039: Wer die Schlüssel hält, hält die Abhängigkeit. Wer sie an zentrale Zertifizierungsmonopole vergibt, baut die zentrale IT unter neuem Namen wieder auf. Das EU-D-S vergibt die Schlüssel dezentral über die Truststation-Schlüsselsätze, eingebettet in die WAN-Anonymität – die erzwungene Erneuerung wird zur Gelegenheit, die Architektur richtig zu verteilen, statt sie nur neu zu verschlüsseln.

Energie, Zahlung, Wasser: die physisch-digitalen Säulen

Die vierte Gruppe hängt mit Strom und Geld am engsten an der physischen Welt. Zentrale Stromnetze werden mit dem Fortschreiten der volatilen Energiewende

störanfälliger, nicht robuster. Das EU-D-S setzt auf dezentrale Energie nach den Patentanmeldungen DE102017004870A1 und DE102016002956A1: dezentrale Erzeugung und Regelung, Inselbetrieb, ein Energie-Butler, der Erzeugung und Verbrauch im Häuserblock ausgleicht. Beim Zahlungsverkehr hat der SWIFT-Ausschluss Russlands 2022 gezeigt, dass zentrale Clearing-Systeme auch als Waffe eingesetzt werden. Das eigene EU-D-S-Zahlungssystem mit der Instant-Payment-Geldbörse macht das Geld wieder zu dem, was Bargeld immer war: etwas im physischen Besitz des Nutzers – einschließlich einer elektronischen Wertbörse, die auch bei Stromausfall funktioniert.

Der Juli 2026 hat der Liste ein Feld hinzugefügt, das sonst gern vergessen wird: Wasser. In den USA wurden mehr als dreißig Wasserwerke eines Bundesstaats und Systeme in einem Dutzend weiterer Staaten koordiniert cyberangegriffen. [39,40] Wasser ist und bleibt eine physische Abhängigkeit: Dezentrale Digitalisierung kann sie nicht ersetzen, aber abfedern – dezentrale Wasserzellen mit lokaler Regelung, Überwachung am Ort, Rückgrat in der Nachbarschaft. Die vollständige Antwort gehört zum Autarkie-Dreiklang Energie–Wasser–Ernährung, dem Finale dieser Reihe 2045.

Die Ehrlichkeitsregel: Ersetzen oder abfedern

Diese Studie verzichtet darauf, dezentrale Digitalisierung zum Allheilmittel zu erklären, denn sie trennt zwei unterschiedliche Wirkungen. Voll ersetzbar durch dezentrale Digitalisierung sind: zentrale IT, zentrale Daten, zentrale Warnung samt Warnkanälen, Notruforganisation, Spezialistenmonopole, die Schlüssel- und Kryptographie-Verwaltung – und die Zeit, wenn das System von Anfang an ohne sie entworfen wird. Nur abfedern lässt sich die physische Schicht: Satelliten, Seekabel, Stromnetze, Wasserleitungen. Hier braucht es weiterhin parallele physische Strukturen – eigene Satellitensysteme, Kabel-Redundanz, dezentrale Energieanlagen, dezentrale Wasserzellen. Aber das EU-D-S-Design entscheidet darüber, wie schwer ein Ausfall wiegt. **Dezentrale Digitalisierung ersetzt kein einziges Kabel – aber sie nimmt jedem Kabelbruch die Katastrophenwirkung.** Eine Gesellschaft, deren Systeme offline arbeiten, nur Metadaten führen und Admin-Kopien halten, erlebt die Drosselung eines Satellitensystems als Verlangsamung, nicht als Lähmung. Genau das trennt 2039 von 2026: nicht die Abwesenheit von Angreifern, sondern die Abwesenheit einzelner Ziele.

Der Staat baut zentral – die Studie denkt dezentral

Der Kontrast zur Gegenwart ist 2026 sichtbar geworden: Deutschland beschloss ein zehnmilliardenschweres Zivilschutzprogramm, mit landesweiter Schutzraum-Inventur in der NINA-App und einem neuen Zivilschutzkommando; [41] Dänemark legte ein 190-Millionen-Paket für „totale Vorsorge“ auf. [42] Die Rückkehr des Zivilschutzens ist richtig und überfällig. Aber die Architektur dieser Rückkehr ist zentral: eine App, ein Kommando, eine Warnzentrale – genau die Struktur, deren Ausfälle und Angriffe die Beleglage 2024–2026 dokumentiert. Diese Studie

widerspricht dem Zivilschutz nicht; sie ergänzt die eine Ebene, die im staatlichen Wiederaufbau fehlt: die Breite. Ein Staat kann Schutzräume inventarisieren, aber er kann Nachbarschaften nicht verordnen. Er kann Warnungen aussenden, aber er kann nicht garantieren, dass sie die Menschen erreichen, wenn die eine App ausfällt oder gehackt wird. Was 2039 resilient macht, ist die Verbindung aus beidem: dem staatlichen Rückgrat und der dezentralen Vernetzung, die auch dann funktioniert, wenn das Rückgrat getroffen wird.

Ausblick

Resilienz ist am Ende nicht nur eine technische, sondern eine gesellschaftliche Eigenschaft: Eine Gesellschaft, die jeden Bürger über Truststation-Nummern erreichen kann, ist auch im demografischen Wandel widerstandsfähig. Der Weg dorthin ist keine Revolution, sondern eine Wachstumskurve – von rund der Hälfte der Bevölkerung im EU-D-S im Jahr 2038 bis zu dem ersten Land, das 2045 seine Verwaltung vollständig im EU-D-S organisiert: wahrscheinlich die Ukraine, deren Wiederaufbau das EU-D-S von Anfang an als Rückgrat dient. Das ist die Brücke zum nächsten Jahresblock – Teilhabe im Alter 2040.

Fußnoten

[1] AFP (14.10.2026): Ukraine meldet verbesserten Starlink-Zugang, bestätigt weiter geltende Tempo-Limits von 161 km/h für bewegliche Terminals.

[2] AFP (16.10.2026): EU unterstützt die Ukraine, kann die Lücke nicht schließen; IRIS²-Start 2029, voll operativ etwa ein Jahr später.

[3] Litauen (2026): Warnung vor russischem GPS-Spoofing – Störsender in Kaliningrad von drei auf 36 Antennen gestiegen, Reichweite bis 450 km.

[4] Euronews (24.08.2026): Landesweite GPS-Störungen in Polen – Telefone, Drohnen und Schiffe „blind“.

[5] Congressional Research Service (11.08.2026): Satellitennavigations-Störung als fester Bestandteil russischer hybrider Kriegsführung.

[6] Balticconnector (10/2023): Beschädigung von Gas- und Datenkabel zwischen Finnland und Estland.

[7] C-Lion1 (11/2024): Seekabel Finnland–Deutschland beschädigt; deutscher Verteidigungsminister: „Sabotage“.

[8] tagesschau (Juli 2024): Globale CrowdStrike-Störung; BSI bestätigt Betroffenheit kritischer Infrastruktur in Deutschland.

[9] Bericht zur IT-Störung der Charité: Aufnahme, Behandlung und Dokumentation betroffen.

[10] UN/ITU: Warnung vor einer „digitalen Pandemie“ – globale Kettenreaktionen in vernetzten Systemen.

[11] Wikipedia (2026): Amateurfunk-Notkommunikation – unabhängig von terrestrischer Infrastruktur, keine Choke Points, Batteriebetrieb.
https://en.wikipedia.org/wiki/Amateur_radio_emergency_communications

[12] Ailunce (2021): Hurrikan Ida – Funkamateure als letzte funktionierende Meldewege in betroffenen Gebieten. https://www.ailunce.com/blog/ham-radio-emergency-why-noaa-weather-radio-matters

[13] AP (25.10.2026): Starshield-Tempo-Grenzen nach Tagen aufgehoben; UAV-Berater Beskrestnov zur Störung der Abfangmissionen.
https://apnews.com/article/ukraine-russia-war-starlink-musk-satellite-connectivity-0c6e685ee4637529ec64c1d6a902cc94

[14] The Guardian (26.11.2024): „They cannot be jammed“ – Glasfaser-Drohnen in der Ukraine (via DroneXL, 23.04.2025). https://dronexl.co/2025/04/23/fiber-optic-drones-warfare-ukraine/

[15] TechUkraine (02.04.2025): Brave1-Großtest mit über 15 Herstellern, Glasfaser-FPVs auf 20-km-Route.
https://techukraine.org/2025/04/02/ukraines-invisible-drones-major-test-sees-fiber-optic-fpvs-hit-20-km-range-bypassing-ew-threats/

[16] Battle Policy (18.08.2026): Ukrainisches Verteidigungsministerium: mehr als 70 KI-/Maschinensicht-Systeme; Ziel Maschinensicht in jeder Frontdrohne.

https://www.battlepolicy.com/ukraine-says-70-plus-ai-systems-help-its-drones-strike-through-russian-jamming/
[17] The Defense Post (19.11.2025): TFL-1-Modul, ca. 100 US-$, autonome Endphase 400–500 m. https://thedefensepost.com/2025/11/19/ai-upgrade-ukrainian-drones/
[18] Ars Technica (Aug. 2026): Auterion/SkyFall-Kooperation, Zielbindung auf 18-US-$-Chip. https://arstechnica.com/ai/2026/08/ukraines-drones-get-ai-upgrades-for-kamikaze-strikes-future-swarm-attacks/
[19] Euromaidan Press (12.06.2026): KI in ukrainischen Middle-Strike-Systemen gegen elektromagnetische Störung. https://euromaidanpress.com/2026/06/12/how-ukraine-is-integrating-ai-into-its-long-range-drone-strike-system/
[20] The Economist/Mint (24.09.2024): Zvook, ca. 500 US-$ je Sensor, 5–7 km Reichweite. https://www.livemint.com/global/ukraine-air-defense-acoustic-detection-systems-drone-detection-technology-military-innovation-ukraine-tech-start-ups-11727266490636.html
[21] Tom Cooper (2024): Zvook als „riesiges, dezentrales passives Sonar“. https://xxtomcooperxx.substack.com/p/of-tech-industry-and-air-defence
[22] Defence Blog (Okt. 2026): Zvook testet erstmals mobile Sensoren auf der NATO-Übung BATT26 in Lettland. https://defence-blog.com/ukrainian-firm-tests-mobile-version-of-its-acoustic-drone-detector/
[23] WIRED (06.03.2025): Ukrainische Telekom-Improvisationen, u. a. Handys auf Stangen als Luftlagensensoren (via HeadTopics). https://us.headtopics.com/news/if-ukraine-loses-starlink-here-are-the-best-alternatives-66703134
[24] Small Wars Journal (13.07.2026): Analyse der ePPO-Bürger-Sensor-App. https://smallwarsjournal.com/2026/07/13/citizen-sensors/
[25] Express (2022): ePPO Observer von Technari – Zielangaben per Knopfdruck an die Flugabwehr. https://www.express.co.uk/news/world/1685240/ukraine-iran-drones-smartphone-ePPO-Observer-app-russia-invasion-latest-news-ont
[26] Forbes (12.02.2024): Pokrova – landweites Spoofing-System gegen die Shahed-Navigation. https://www.forbes.com/sites/davidhambling/2024/02/12/ukraines-pokrova-spoofing-system-tells-shaheds-to-get-lost/
[27] The Defense Post (05.12.2024): 95 von 188 Shaheds per Spoofing umgeleitet (nach Le Monde). https://thedefensepost.com/2024/12/05/ukraine-spoofs-shahed-drones/
[28] Futurism (Okt. 2026): Sam Altman im Cheeky-Pint-Podcast – lokale Inferenz aus „globaler Allokationsperspektive“ „quite terrible“; Kontext: Intel-Kurssturz ~30 %, Speicherpreise, Leiterplatten bis Ende 2030 ausgebucht. https://futurism.com/artificial-intelligence/sam-altman-hates-local-ai-models-computers
[29] Nature (2025): GPS-Zeitverteilung zunehmend verwundbar – Timing als kritische Infrastruktur. https://www.nature.com/articles/d41586-025-02921-z
[30] Business Sun Times (2026): GPS als Weltzeitgeber für Finanzmärkte und Stromnetze; Zeitstempel-Pflicht für Transaktionen. https://businesssuntimes.com/gps-now-worlds-timekeeper-for-financial-markets-power-grids/
[31] GISAD: Projekt „das EI“ – Best-Practice-Dokumentation der ohne Zeitangabe programmierten Entwicklungen (Helligkeit, Bewegung, PV-Ertrag). Online: https://gisad.eu/best-practice/projekt-das-ei/ (abgerufen 03.11.2026). https://gisad.eu/best-practice/projekt-das-ei/
[32] BBC (2026): Notfall-Apps der Ukraine und Russlands gehackt – gefälschte Strahlen- und Kriegsalarme. https://www.bbc.com/news/live/cm4g1yjxv38gt
[33] Rumänien (25.04.2026): Gefälschte RO-ALERT-Meldungen in sozialen Netzwerken, Ziel: Panik. https://www.oradesibiu.ro/2026/04/25/fake-news-periculos-mesaj-ro-alert-fals-despre-rapiri-circula-pe-facebook-si-whatsapp/
[34] DISA (2026): Gefälschte Evakuierungsbefehle und KI-Bilder bei den Waldbränden in British Columbia. https://disa.org/misinformation-regarding-british-columbia-wildfires-circulates-online/
[35] Harvest now, decrypt later: Sammlung verschlüsselten Materials zur späteren Entschlüsselung durch Quantenrechner. https://buaq.net/go-424801.html
[36] OpenSSL Corporation (2026): US-Anordnung vom 22.06.2026 – Post-Quanten-Kryptographie für kritische Systeme bis 31.12.2030, Signaturen bis 31.12.2031. https://openssl-corporation.org/blog/post-quantum-cryptography-now-has-deadlines.html
[37] BSI: TR-02102-1 (Januar 2026) – Enddaten klassischer Kryptographie: 2030 (höchstkritisch), 2031 (Schlüsselaustausch), 2035 (nur-klassische Signaturen). https://postquantum.com/security-pqc/germany-bsi-pqc-deadlines-2030/
[38] Sinevis (12.10.2026): BMI, BMDS und BSI veröffentlichen nationale Umsetzungsrichtlinie zur

Post-Quanten-Migration. https://sinevis.com/pqc-migration-readiness-2026/

[39] Water Online (2026): Mehr als 30 Wasserwerke in Minnesota und Systeme in einem Dutzend Staaten koordiniert angegriffen.
https://www.wateronline.com/doc/water-utilities-seek-resources-to-combat-growing-cyberattack-threat-0001

[40] Forbes (01.08.2026): FBI zu Cyberangriffen auf Wassersysteme; EPA: 70 % der geprüften Systeme mit Mängeln.
https://www.forbes.com/sites/steveweisman/2026/08/01/will-the-cyberattacks-on-water-systems-in-7-states-be-a-wakeup-call/

[41] AFP (18.05.2026): Deutschland plant 10 Mrd. € Zivilschutz – Schutzraum-Inventur in der NINA-App, neues Zivilschutzkommando.

[42] AFP (20.02.2026): Dänemark: 1,2 Mrd. Kronen (190 Mio. $) für „totale Vorsorge“ nach nordischem Vorbild.

Impressum / Legal Notice
DE
Global Institute for Structure relevance,
Anonymity and Decentralization i.G.

Initiator
Olaf Berberich

Breiten Dyk 14
47803 Krefeld
Telefon : 02151-3872601
Mail: infoh@finders.de
Web: www.gisad.eu
EU-Register Nr. **244298340978-40**

Complainant at the Federal Constitutional Court:
- 1 BvR 227/23 - , -1 BvR 1640/24-, -1 BvR 1641/24-,
-2 BvR 907/24 -, -1 BvR 1426/25 -, -2 BvR 1668/25-
-1 BvR 91/26 -

Datenschutz

Die Texte der Studien basieren auf automatischen Recherchen im Internet und werden mithilfe der KI Mistral.ai optimiert und übersetzt. Dabei werden Quellen automatisch ermittelt. Alle Angaben werden sorgfältig geprüft. Sollte sich im Einzelfall doch einmal ein Fehler einschleichen, wären wir für jeden Hinweis dankbar.
Bitte beachten Sie dass von facebook.de, WhatsUp und weiteren Portalen Accounts unter meinem Namen angelegt sind, welche ich nicht pflege, aber auch nicht löschen kann. Außer über E-Mail können Sie GISAD über XING oder Linkedin erreichen!

GISAD für ein starkes digitales Europa!
Mit Hilfe der EU die vordigitalen Errungenschaften erhalten!

GISAD