Detailkonzept Cyberresilienz und digitale Verwundbarkeit

Cybersecurity als Gesellschaftsschutz und Freiheitsbedingung

Autorin: Natalie Weber
Referenz: Wirkungsökonomie
Portal: Rang 16 - Sicherheit, Resilienz und globale Kooperation
Version: 1.0
Status: Detailkonzept - Langfassungsentwurf v1.0
Stand: 24. Mai 2026

Wirkung ist neutral und relational. Ziel ist positive Netto-Wirkung für Mensch, Planet und Demokratie.

Untertitel: Cybersecurity als Gesellschaftsschutz und Freiheitsbedingung

Autorin: Natalie Weber

Referenz: Wirkungsökonomie

Portal: Rang 16 - Sicherheit, Resilienz und globale Kooperation

Version: 1.0

Status: Detailkonzept - Langfassungsentwurf v1.0

Stand: 24. Mai 2026

Executive Summary

Cyberresilienz schützt nicht nur Systeme, sondern Verwaltung, Gesundheit, Märkte, Vertrauen, öffentliche Wahrheit und demokratische Handlungsfähigkeit.

Begriffliche Leitlinie

Für Rang 16 gilt der führende Begriffsleitfaden der Wirkungsökonomie. Wirkung ist neutral und relational. Sie beschreibt die tatsächliche Veränderung von Zuständen und kann positiv, negativ oder neutral sein. Bewertet wird Wirkung am Referenzrahmen der SDGs, der Agenda 2030 und SDG+. Ziel der Wirkungsökonomie ist positive Netto-Wirkung für Mensch, Planet und Demokratie.

Sicherheit wird deshalb nicht als bloße Abwehr, Kontrolle oder militärische Stärke verstanden. Sicherheit ist ein Wirkungszustand: Menschen bleiben geschützt, lebenswichtige Funktionen bleiben verfügbar, demokratische Korrekturfähigkeit bleibt erhalten, Infrastruktur bleibt belastbar, Information bleibt vertrauenswürdig und politische Entscheidungen bleiben rechtsstaatlich begrenzt.

Resilienz bedeutet nicht Abschottung. Resilienz bedeutet Lern-, Anpassungs- und Kooperationsfähigkeit unter Stress. Eine resiliente Gesellschaft kann Störungen aufnehmen, Grundfunktionen aufrechterhalten, Schaden begrenzen, aus Krisen lernen und ihre Freiheit bewahren.

1. Ausgangslage und Problemstellung

Digitale Verwundbarkeit entsteht nicht erst durch einen erfolgreichen Angriff. Sie entsteht durch Abhängigkeit ohne Ausweichfähigkeit, unklare Zuständigkeiten, veraltete Systeme, schwache Datenintegrität und fehlende analoge Rückfallebenen.

Die zentrale Schwäche klassischer Steuerung besteht darin, dass Risiken nach Zuständigkeiten, Schadensarten oder politischen Ressorts sortiert werden. Wirkung entsteht aber über Grenzen hinweg. Eine Störung kann technische, soziale, ökologische, finanzielle, demokratische und psychologische Folgen zugleich haben. Deshalb braucht Rang 16 eine Wirkungsarchitektur, die Kopplungen sichtbar macht.

2. Wirkungsökonomische Leitfrage

Ein Cyberangriff auf eine Kommune wirkt auf Bürgervertrauen, Verwaltungsgeschwindigkeit, Sozialleistungen, Gesundheitsversorgung, Medienkommunikation, politische Schuldzuweisung und Sicherheitsempfinden. Die Wirkungsökonomie bewertet Cyberrisiken deshalb nach Zustandsveränderung, nicht nur nach technischem Schweregrad.

Diese Leitfrage verhindert zwei Fehlsteuerungen. Erstens verhindert sie die Verengung auf Symbolik: Nicht jede harte Maßnahme erzeugt Sicherheit. Zweitens verhindert sie Kontrollüberschuss: Nicht jede Risikoquelle rechtfertigt Überwachung oder Zentralisierung. Entscheidend ist positive Netto-Wirkung für Mensch, Planet und Demokratie.

3. Fachliche Unterbereiche

- Governance nach NIST CSF 2.0 und NIS2-Anschluss
- Datenintegrität
- Backup und Wiederherstellung
- kommunale Cyberresilienz
- Schutz von Krankenhäusern und Versorgung
- Wirkungsdatenräume
- digitale Rückfallebenen

Jeder Unterbereich braucht Daten, Verantwortlichkeiten, Schutzstandards, Finanzierungslogik, Beteiligung und Evaluation. Eine Maßnahme gilt nicht deshalb als wirksam, weil sie beschlossen wurde. Sie gilt erst dann als wirksam, wenn Zustände sich nachvollziehbar verbessern oder Risiken nachweisbar sinken.

4. Daten- und Bewertungslogik

Für dieses Detailkonzept werden folgende Datenebenen empfohlen:

- Strukturindikatoren: Vorhandensein von Plänen, Zuständigkeiten, Standards, Rückfallebenen und Ressourcen.
- Leistungsindikatoren: Reaktionszeiten, Wiederherstellungszeiten, Versorgungsreichweite, Datenqualität und Beteiligung.
- Wirkungsindikatoren: tatsächliche Verringerung von Verwundbarkeit, Folgeschäden, Ausfallwirkung, Vertrauensverlust und sozialer Belastung.
- Gerechtigkeitsindikatoren: Schutz vulnerabler Gruppen, Barrierefreiheit, Mehrsprachigkeit, soziale Abfederung und Grundrechtswirkung.
- Demokratieindikatoren: Transparenz, Rechenschaft, Korrektur, Rechtsmittel, Medienqualität und Beteiligung.

Die Bewertung folgt dem Nichtkompensationsprinzip. Ein gutes Ergebnis bei technischer Verfügbarkeit darf schwere Defizite bei Grundrechten, Barrierefreiheit, Datenintegrität oder Schutz vulnerabler Gruppen nicht unsichtbar machen. Umgekehrt darf ein hoher Beteiligungsgrad technische Verwundbarkeit nicht schönrechnen.

5. Beispielhafte Scorecard

Wirkungsfeld	Prüffrage	Datenquelle	Bewertung
Mensch	Wer ist bei Ausfall zuerst betroffen?	Sozialdaten, Einsatzdaten, Befragungen	-3 bis +3
Planet	Senkt die Maßnahme ökologische Verwundbarkeit?	Klima-, Wasser-, Energie- und Flächendaten	-3 bis +3
Demokratie	Bleiben Rechte, Vertrauen und Korrektur erhalten?	Rechtsprüfung, Beteiligung, Medienmonitoring	-3 bis +3
Infrastruktur	Gibt es Rückfallebenen und Wiederherstellung?	Betreiberberichte, Audits, Übungen	-3 bis +3
Daten	Sind Daten korrekt, sicher und nutzbar?	Audit, DII, Cyberberichte	-3 bis +3

6. Berechnungslogik und Bewertungsmodell

Die Berechnungslogik dieses Detailkonzepts folgt drei Ebenen. Erstens wird die Kritikalität bestimmt: Welche Funktion, welches System oder welcher Wirkungsraum ist betroffen? Zweitens wird die Verwundbarkeit bestimmt: Wie wahrscheinlich ist eine Störung, wie stark ist die Abhängigkeit, welche Ersatzwege bestehen und welche Gruppen sind besonders verletzlich? Drittens wird die Ausfallwirkung bestimmt: Welche Zustände verändern sich bei Störung, Verzögerung, Manipulation oder Verlust?

Eine einfache Formel für die Vorprüfung lautet:

Wirkungsrisiko = Kritikalität x Verwundbarkeit x Ausfallwirkung x Dauer x Ungleichheitsfaktor

Diese Formel ist keine starre mathematische Endbewertung. Sie dient als strukturierte Leselogik. Kritikalität beschreibt die Bedeutung einer Funktion für Mensch, Planet und Demokratie. Verwundbarkeit beschreibt technische, soziale, ökologische, rechtliche und organisatorische Schwächen. Ausfallwirkung beschreibt die tatsächliche Zustandsveränderung. Dauer beschreibt, ob eine Störung Minuten, Tage, Wochen oder Jahre wirkt. Der Ungleichheitsfaktor macht sichtbar, ob bestimmte Gruppen stärker betroffen sind: Kinder, ältere Menschen, Menschen mit Behinderung, Menschen in Armut, Menschen mit Pflegebedarf, Menschen ohne digitale Zugänge, Menschen mit unsicherem Aufenthaltsstatus oder Menschen in besonders belasteten Regionen.

Die Bewertung erfolgt auf einer Skala von -3 bis +3. -3 steht für hoch destruktive Wirkung, -2 für schädliche Wirkung, -1 für schwache oder riskante Wirkung, 0 für neutral oder unzureichend belegt, +1 für stabilisierende Wirkung, +2 für sehr gute Resilienzwirkung und +3 für transformative Wirkung. Transformativ ist eine Maßnahme erst dann, wenn sie nicht nur ein einzelnes Risiko senkt, sondern die Systemlogik verbessert: bessere Rückkopplung, geringere Abhängigkeit, höhere Lernfähigkeit, fairere Lastenverteilung und demokratische Korrektur.

Das Nichtkompensationsprinzip gilt auch hier. Eine Infrastruktur kann nicht als resilient gelten, wenn sie technisch verfügbar ist, aber vulnerable Gruppen ausschließt. Ein Cyberprogramm kann nicht als positiv gelten, wenn es Sicherheit erhöht, aber Grundrechte unverhältnismäßig beschneidet. Eine Krisenstrategie kann nicht als gut gelten, wenn sie schnelle Reaktion ermöglicht, aber Vertrauen zerstört. Rang 16 verlangt deshalb eine Mindestlogik: kein zentraler Wirkungsbereich darf unter die rote Linie fallen.

7. Datenquellen und Nachweislogik

Für die praktische Umsetzung werden Daten nicht neu erfunden, sondern aus bestehenden Quellen zusammengeführt. Dazu gehören Betreiberberichte, kommunale Lagebilder, Katastrophenschutzpläne, Cyberaudits, KRITIS-Meldungen, Gesundheitsdaten in aggregierter Form, Wetter- und Klimadaten, Wasser- und Energiedaten, Sozialraumprofile, Einsatzstatistiken, Bürgerbefragungen, Wissenschaftsdaten, Versicherungsdaten und offene Frühwarninformationen.

Die Wirkungsökonomie unterscheidet dabei zwischen Rohdaten, Bewertungsdaten und Steuerungsdaten. Rohdaten beschreiben Zustände. Bewertungsdaten ordnen sie in Bezug auf Mensch, Planet und Demokratie ein. Steuerungsdaten lösen Entscheidungen aus: Investitionen, Priorisierung, Warnung, Training, Sanierung, Rückfallplanung, Förderung oder regulatorische Korrektur.

Datenqualität ist selbst ein Sicherheitsfaktor. Schlechte Daten erzeugen falsche Prioritäten. Fehlende Daten erzeugen blinde Flecken. Manipulierte Daten erzeugen Scheinsicherheit. Deshalb braucht Rang 16 einen Datenintegritätsstandard: Herkunft, Aktualität, Plausibilität, Zugänglichkeit, Datenschutz, Revisionssicherheit, Versionierung und unabhängige Prüfung müssen dokumentiert werden.

8. Umsetzungsebenen

Die Umsetzung erfolgt auf fünf Ebenen. Auf der staatlichen Ebene braucht es Rechtsrahmen, Mindeststandards, Finanzierung, Datenschutz und Krisenkoordination. Auf der kommunalen Ebene braucht es Sozialraumprofile, lokale Anlaufstellen, Warnwege, Übungen, Beteiligung und konkrete Rückfallebenen. Auf der Betreiber- und Unternehmensebene braucht es Risikoanalysen, Notfallprozesse, Lieferkettenresilienz, Cyberresilienz und Transparenz. Auf der zivilgesellschaftlichen Ebene braucht es Nachbarschaft, Ehrenamt, Kultur, Vereine, Beratung, Medienkompetenz und Teilgabe. Auf der internationalen Ebene braucht es Daten- und Frühwarnkooperation, faire Partnerschaften und Schutz kritischer Lieferketten.

Alle Ebenen dürfen nicht isoliert arbeiten. Resilienz entsteht in der Kopplung. Ein kommunaler Hitzeplan wirkt nur, wenn Gesundheitsdienste, Pflege, Wohnungswirtschaft, Energieversorgung, Wasser, Nachbarschaft und Kommunikation zusammenspielen. Ein Cyberplan wirkt nur, wenn Verwaltung, Anbieter, Bürgerdienste, Krankenhäuser, Zahlungswege und analoge Alternativen verbunden sind. Eine Außenpolitik der Resilienz wirkt nur, wenn Klima, Rohstoffe, Lieferketten, Daten, Gesundheit und demokratische Stabilität gemeinsam betrachtet werden.

9. Beispiele für Wirkungslogik

Beispiel A: Eine Kommune richtet ein neues Warnsystem ein. Klassisch würde geprüft, ob die Technik funktioniert. Wirkungsökonomisch wird zusätzlich geprüft: Erreicht die Warnung Menschen ohne Smartphone? Ist sie mehrsprachig? Gibt es barrierefreie Formate? Gibt es lokale Anlaufstellen? Wissen Pflegeeinrichtungen, Schulen, Kitas und Krankenhäuser, was zu tun ist? Gibt es Rückmeldeschleifen nach Übungen? Nur dann entsteht positive Netto-Wirkung.

Beispiel B: Ein Betreiber kritischer Infrastruktur investiert in digitale Steuerung. Klassisch kann das Effizienz erhöhen. Wirkungsökonomisch muss geprüft werden, ob neue digitale Abhängigkeiten entstehen, ob analoge Notfallprozesse erhalten bleiben, ob Daten manipulationssicher sind, ob Personal geschult ist und ob Ausfälle gesellschaftliche Folgeschäden erzeugen. Effizienz ohne Rückfallebene kann Verwundbarkeit erhöhen.

Beispiel C: Eine Regierung reagiert auf hybride Risiken mit schärferen Überwachungsinstrumenten. Klassisch kann das als Sicherheit gelten. Wirkungsökonomisch muss geprüft werden, ob Grundrechte, Minderheitenschutz, Pressefreiheit, freie Wissenschaft und demokratische Opposition geschützt bleiben. Sicherheit, die Freiheit zerstört, erzeugt negative Netto-Wirkung.

10. Website-, Download- und Tool-Integration

Für die Website wird dieses Detailkonzept als vollständiger Online-Volltext bereitgestellt. Der PDF-Download erhält Corporate Design, Autorin Natalie Weber, Referenz Wirkungsökonomie, Version, Status und Stand. Die Toolkarte verweist auf eine Demo in Vorbereitung und beschreibt klar, ob es sich um Dashboard, Scorecard, Index, Radar, Planer oder Matrix handelt.

Die Onlinefassung braucht ein mobiles Inhaltsverzeichnis, Druckfunktion, Glossarlinks, Quellenblock, SDG-/SDG+-Block und politische Anschlussfähigkeit. Tabellen müssen mobil lesbar sein. Kein Text darf nur als PDF existieren. Die Wirkung der Website selbst wird daran gemessen, ob sie Orientierung schafft, nicht nur Dokumente ablegt.

11. Umsetzungspfad

1. Bestandsaufnahme der betroffenen Wirkungsräume.
2. Festlegung von Mindeststandards und roten Linien.
3. Pilotierung mit Kommunen, Betreibern, Verwaltung, Zivilgesellschaft und Wissenschaft.
4. Aufbau eines öffentlichen, datenschutzkonformen Dashboards.
5. Jährliche Evaluation mit Korrekturpflicht.
6. Verknüpfung mit Wirkungshaushalt und Wirkungsfonds.
7. Veröffentlichung einer Onlinefassung und eines Downloads.

12. Politische Anschlussfähigkeit

Politische Anschlussfähigkeit und Umsetzungsoptionen

Die Wirkungsökonomie liefert keinen fertigen Parteiprogrammtext. Sie liefert einen Bewertungs- und Steuerungsrahmen. Parteien behalten Ausgestaltungsspielraum: Sie können Sicherheits-, Innen-, Außen-, Digital-, Sozial-, Infrastruktur- und Haushaltspolitik unterschiedlich gewichten. Entscheidend ist, ob die gewählte Politik ihre Wirkung transparent macht, Grundrechte achtet, kritische Funktionen schützt und Korrektur ermöglicht.

Aufgabe der Politik ist es, Risiken nicht zu verdrängen und zugleich keine Kontrolllogik zu erzeugen. Ein Sicherheitsstaat versucht, Risiken durch Überwachung und Zentralisierung zu minimieren. Ein Resilienzstaat schützt Handlungsfähigkeit, ohne die offene Gesellschaft zu schließen. Er setzt auf Vorsorge, klare Zuständigkeiten, robuste Infrastruktur, dezentrale Rückfallebenen, verlässliche Kommunikation, Rechtsstaatlichkeit und

demokratische Kontrolle.

Politische Rahmenbedingungen sind: klare Risiko- und Zuständigkeitsarchitektur, transparente Daten, Schutz kritischer Einrichtungen, digitale und analoge Notfallfähigkeit, föderale Koordination, kommunale Umsetzung, soziale Abfederung, unabhängige Evaluation und Beteiligung der Bevölkerung. Zielkonflikte müssen offen benannt werden: Sicherheit und Freiheit, Tempo und Rechtsstaat, Zentralisierung und lokale Handlungsfähigkeit, Geheimschutz und Transparenz, Prävention und Kosten, internationale Kooperation und Souveränität.

Evaluation und Korrektur sind Pflicht. Sicherheits- und Resilienzpolitik muss prüfen, ob Maßnahmen tatsächlich Verwundbarkeit senken, Versorgung sichern, Vertrauen stärken, Freiheit schützen und Folgeschäden reduzieren. Nicht eingetretene Katastrophen sind keine Wirkungslosigkeit. Sie können Ergebnis gelungener Prävention sein.

13. Zielkonflikte und Schutzgrenzen

Zentrale Zielkonflikte sind: schnelle Reaktion versus Rechtsstaatlichkeit, Transparenz versus Sicherheitsinteressen, Zentralisierung versus Dezentralität, Effizienz versus Redundanz, Datenzugang versus Datenschutz, Sicherheitslogik versus offene Gesellschaft und nationale Vorsorge versus internationale Kooperation. Diese Zielkonflikte dürfen nicht verdeckt werden. Sie müssen methodisch dokumentiert und demokratisch entschieden werden.

14. SDG- und SDG+-Bezug

SDG- und SDG+-Bezug

Rang 16 berührt mehrere SDGs direkt: SDG 3 Gesundheit und Wohlergehen, SDG 6 Wasser, SDG 7 Energie, SDG 9 Industrie, Innovation und Infrastruktur, SDG 11 nachhaltige Städte und Gemeinden, SDG 13 Klimaschutz, SDG 16 Frieden, Gerechtigkeit und starke Institutionen sowie SDG 17 Partnerschaften. Sicherheit und Resilienz sind keine Zusatzthemen, sondern Schutzbedingungen für die Erreichung dieser Ziele.

Der SDG+-Bezug ist zentral. Demokratiequalität, Medienqualität, Rechtsstaatlichkeit, Diskursfähigkeit, institutionelles Vertrauen, gesellschaftlicher Zusammenhalt, digitale Selbstbestimmung und Datenintegrität entscheiden darüber, ob eine Gesellschaft Krisen bewältigen kann. Ohne diese Dimensionen können SDGs formal gemessen werden, während ihre politischen Voraussetzungen erodieren.

SDG+ ist keine offizielle UN-Kategorie. Es ist die transparente Erweiterung der Wirkungsökonomie für jene demokratischen und medialen Bedingungen, ohne die die SDGs nicht stabil erreichbar sind.

15. Quellen und Glossar

Quellen- und Anschlussrahmen

Interne WÖk-Anschlüsse:

- Führender Begriffsleitfaden der Wirkungsökonomie, Version 1.0, Stand 21. Mai 2026.
- Natalie Weber: Die neue Ordnung des Wohlstands, Arbeitsfassung 2026, Kapitel 65 Resilienzstaat, Kapitel 66 Sicherheitsarchitektur, Kapitel 84 Cyberresilienz, Kapitel 95 Globale Resilienz, Sicherheit und Kooperation.
- Natalie Weber: Systemmodell der Wirkungsökonomie, 2025, Module Außenpolitik und Sicherheitspolitik, Bundeswehr und alternative Dienstpflicht, Katastrophenschutz und Systemresilienz, Demokratie-Schutzarchitektur, Digitalisierungsindikatoren.

Externe Anschlussquellen:

- United Nations Office for Disaster Risk Reduction: Sendai Framework for Disaster Risk Reduction 2015-2030.
- OECD: Good Governance for Critical Infrastructure Resilience.
- OECD: Recommendation on the Governance of Critical Risks.

• Europäische Union: Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen.
• Europäische Union: Richtlinie (EU) 2022/2555, NIS2-Richtlinie.
• Europäische Kommission: Preparedness Union Strategy, 2025.
• NATO: Resilience, civil preparedness and Article 3.
• NIST: Cybersecurity Framework 2.0, 2024.
• Bundesamt für Sicherheit in der Informationstechnik: Lage der IT-Sicherheit in Deutschland, 2025.