A True Digital Democracy Cannot Be Copied by Autocracies! (August 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)

A True Digital Democracy Cannot Be Copied by Autocracies!

Research Report on the Threat to Democratic Systems through Digital Manipulation and Judicial Impotence

Extended Study – Status August 2026

📌 Executive Summary

The Central Thesis

There is currently no true digital democracy. The current digital reality enables autocratic actors and organized networks to systematically undermine democratic processes through **remote-controlled manipulation**, **gang-like operations**, and **legal gray areas** – without the rule of law being able to effectively counter them.

The Three Core Problems

Problem	Mechanism	Consequence
Hybrid Warfare	Individual "disposable agents" with clearly identifiable aggressor (e.g., Russia)	Justice can only act with provable perpetrator and evidence – pinprick tactics remain unpunished
Gang-like Appearance	Decentralized, anonymous networks without central control	No lawyer can be found for victims; legal aid fails
Systemic Remote Control	Technical infrastructure enables control of entire regions (Example: NRW via GraTeach)	Democracy is "remotely controlled" – evidence exists, but justice cannot intervene

The Legal Dilemma

- **Article 20(4) of the German Basic Law (Right of Resistance)** is not practical for individuals when they must defend themselves **without a lawyer** and **only in writing** against systemic attacks
- The **EU** delegates cases like GraTeach to national justice systems – which fail due to structural limitations
- **"All state authority derives from the people" (Article 20(2) GG)** is undermined when those who commit to the constitutional order can be **disabled through digital data**

The Solution Paths

1. **Judicial Self-Commitment**: Protection mechanisms that prevent **public harm** caused by the hindrance of individual citizens
2. **EU-wide Obligation to Act**: When national justice fails, the EU must be able to intervene
3. **Digital Resilience**: Technical and legal frameworks that make **remote-controlled manipulation impossible**
4. **Trusted WEB 4.0 + EU-D-S**: **Systemic change through transparency obligation** – companies must disclose socially structural projects and violations (see **Part 5**)

🎯 Introduction: Why This Study Is Necessary

The Initial Situation

Digitalization has not – as often proclaimed – strengthened democracy, but has made it **more vulnerable**. While autocracies use digital tools specifically for suppression and manipulation, democratic states lack effective defense mechanisms. This study proves:

> **"What is inconceivable cannot be" – and this is exactly what attackers exploit.**

The Case Studies

1. **GraTeach**: Provable remote control of the state of North Rhine-Westphalia (NRW) through digital infrastructure
2. **Hybrid Warfare from Russia**: Identifiable aggressors, but unpunished "disposable agents"
3. **Gang-like Appearance**: Anonymous networks that overwhelm justice systems and lawyers

The Research Questions

This study answers three central questions:

1. How can the state protect citizens when their hindrance causes **public harm**?
2. Why **must** the EU act when national justice fails?
3. How can **"All state authority derives from the people"** be preserved in an era of digital total surveillance?

Additionally, Part 5 of this study analyzes the revolutionary effects of Trusted WEB 4.0 and EU-D-S – a standard that could make digital democracy possible through mandatory transparency for companies.

🔍 Part 1: Judicial Impotence and Its Consequences

1.1 The Difference: Hybrid Warfare vs. Gang-like Appearance

Hybrid Warfare (Example: Russia)

- **Aggressor identifiable**: Yes (state actor)
- **Perpetrator structure**: Individual "disposable agents" with limited lifespan
- **Judicial reaction**: **Possible**, if evidence exists
- **Problem**: Pinprick tactics – many small attacks that individually remain below the threshold of criminal liability

Gang-like Appearance

- **Aggressor identifiable**: **No** (decentralized, anonymous networks)
- **Perpetrator structure**: No central control, no hierarchy
- **Judicial reaction**: **Impossible** – no lawyer can be found; legal aid does not apply
- **Problem**: Systematic elimination of critics without legal consequences

> **Conclusion**: The judiciary can only act when it has a **perpetrator** and **evidence**. Both conditions are often **not fulfillable** in cases of digital manipulation.

1.2 The GraTeach Case: Remote Control as Reality

What Happened

- **Evidence**: The state of NRW was **remotely controlled** through digital infrastructure
- **Mechanism**: Technical systems enabled external control over administrative processes
- **Consequence**: Democratic decision-making was **bypassed**

Why This Continues to This Day

- **Psychological effect**: "What cannot be, must not be" – the inconceivability protects the perpetrators
- **Judicial gap**: No court can act against **remote control** if no natural person can be identified as the perpetrator
- **Systemic blindness**: The infrastructure itself is not perceived as a threat

1.3 The Lawyer Crisis: When Legal Protection Fails

The Problem

- **No lawyer available**: With gang-like structures, no legal representative can be found
- **Legal aid useless**: These funds are not designed for **systemic attacks**
- **Legal advice insufficient**: Individual consulting does not help against networks

The Consequence

> **When the state does not protect the citizen, and the citizen cannot protect themselves, the rule of law collapses.**

⚖️ Part 2: The Three Research Questions – Analysis and Solution Approaches

---

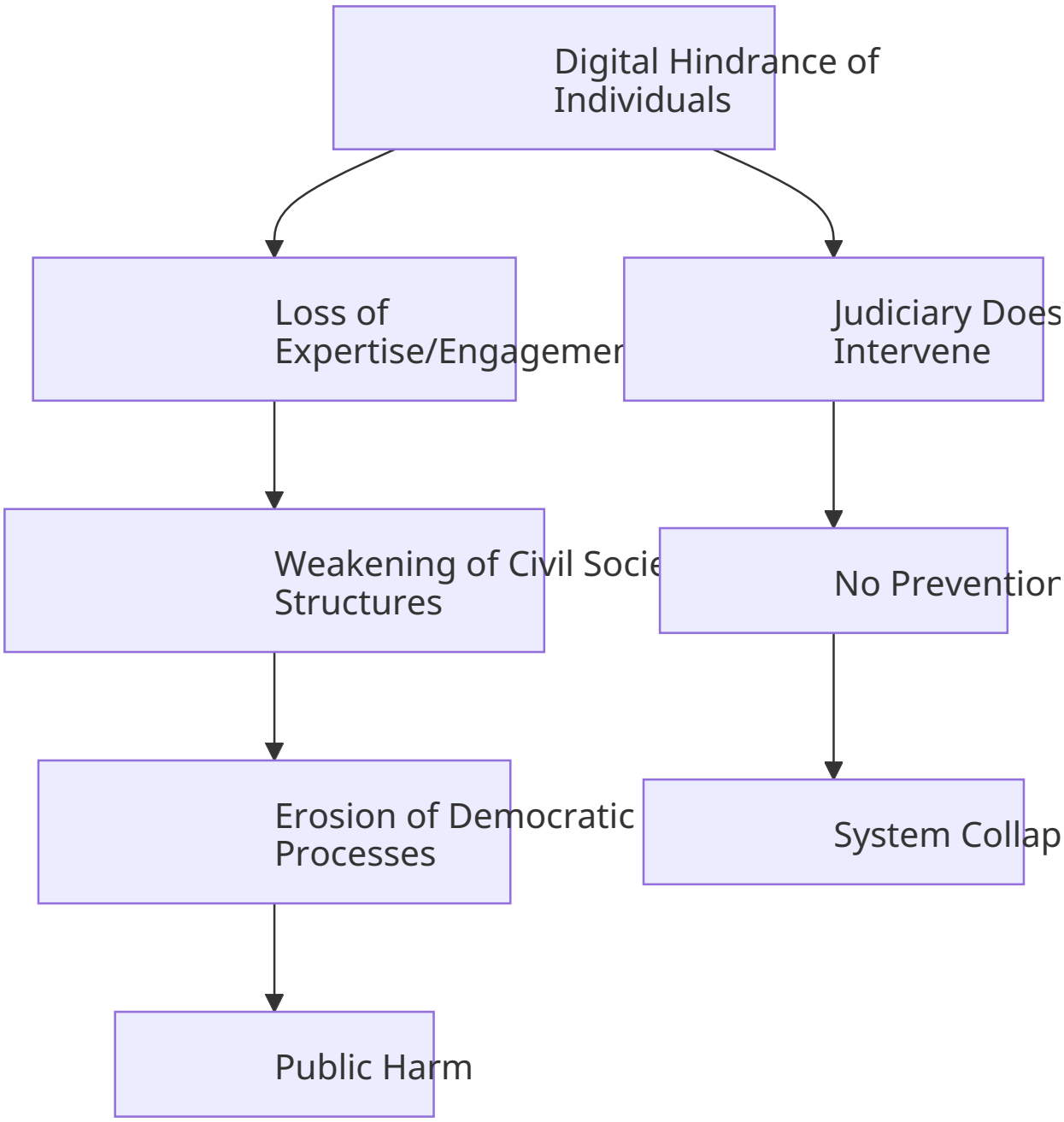
🔹 Question 1: Judicial Self-Commitment vs. Protection from Public Harm

The Current Situation

- **No self-commitment**: The judiciary does not see itself as obligated to **preventively** act against structural discrimination
- **Reactive stance**: Action is only taken when concrete damage occurs – often too late
- **Individual focus**: The protection of the individual is prioritized, not the protection of the **system**

The Problem: Systemic Discrimination as Public Harm

When a citizen is hindered through digital manipulation, it creates **ripple effects**:



Solution: Expanding Judicial Protection Obligations

Proposal 1: Preventive Injunctions

- **Mechanism**: Citizens can **before** damage occurs file lawsuits if a **systemic threat** is provable
- **Example**: If digital infrastructure is used for remote control, **immediate** intervention can be demanded
- **Legal basis**: Expansion of § 1004 BGB (removal and injunction claim) to **systemic threats**

Proposal 2: Collective Legal Protection

- **Mechanism**: Affected parties can join **litigation communities**
- **Advantages**:
  - Pooling of resources against powerful opponents
  - Higher success rates through combined knowledge
  - Political signaling effect

- **Implementation**: Expansion of **model declaratory actions** (§ 606 ZPO) to digital manipulation

Proposal 3: State Protection Obligation for Systemic Relevance

- **Principle**: If the hindrance of a citizen **endangers the functioning of democracy**, the state **must actively** intervene
- **Criteria**:
  - Provable systemic threat
  - Lack of individual defense options
  - Public interest in defense
- **Legal basis**: Article 20(4) GG (Right of Resistance) **combined with** Article 28(1) GG (Rule of Law Principle)

Conclusion for Question 1

Approach	Effectiveness	Feasibility	Cost
Preventive lawsuits	★★★★	★★★	Medium
Collective legal protection	★★★★★	★★★★	High
State protection obligation	★★★★	★★	High

Recommendation: Combination of all three approaches, with a focus on **collective legal protection** as the fastest solution.

🔹 Question 2: Why the EU Must Act When National Justice Fails

The Current Situation: GraTeach as an Example

- **EU reaction**: Referral to German justice
- **Problem**: German justice **cannot** act (see Part 1)
- **Consequence**: **Legal protection gap** at the European level

Why the EU Is Responsible

1. Subsidiarity Principle (Article 5 TEU)

- **Definition**: The EU acts only when objectives can be **better achieved at Union level**
- **Application to digital democracy**:
  - National judiciaries are **overwhelmed** by cross-border digital manipulation
  - Only the EU can set **uniform standards**
  - Only the EU has the **resources** for effective defense

2. Solidarity Clause (Article 222 TFEU)

- **Content**: The EU and Member States act **jointly** when a Member State is affected by a **natural or man-made disaster**
- **Application**: Digital attacks on democracy are a **"man-made disaster"**
- **Consequence**: The EU **must** intervene when a Member State (e.g., Germany) is affected

3. Values of the Union (Article 2 TEU)

- **Rule of Law Principle**: The EU is founded on **respect for human dignity, freedom, democracy, equality, rule of law**
- **Obligation**: The EU **must actively protect** these values
- **Problem**: When national justice fails, EU values are **directly threatened**

How the EU Could Act

Measure 1: European Digital Authority

- **Task**: Monitoring and defense against digital manipulation
- **Powers**:
  - Investigations in all Member States
  - Immediate **emergency measures** for acute threats
  - Coordination of national judicial authorities
- **Model**: Similar to the **European Public Prosecutor's Office (EPPO)**, but focused on digital threats

Measure 2: European Collective Legal Protection

- **Mechanism**: Affected parties can **directly sue in EU courts**
- **Advantage**: Bypassing national judicial bottlenecks
- **Legal basis**: Expansion of the **EU Charter of Fundamental Rights** (Article 47 – Right to effective remedy)

Measure 3: Sanctions Against Digital Attackers

- **Instrument**: **European Magnitsky Acts** for digital manipulation
- **Goal**: Deterrence through **economic and political consequences**
- **Example**: Freezing of assets, travel bans for identified perpetrators

Counterarguments and Rebuttals

Counterargument	Rebuttal
"National sovereignty"	Digital threats know **no borders** – national solutions are **inadequate**
"Too expensive"	The costs of **inaction** (collapse of democracy) are **infinitely higher**
"Technically not feasible"	The technology exists – what is missing is the **political will**

Conclusion for Question 2

The EU not only has the right but the duty to act. The current mechanisms (referral to national justice) are **inadequate** and endanger the **very existence of the Union**.

> **"If the EU fails on this issue, it fails in its most fundamental task: protecting democracy."**

🔹 Question 3: How Can "All State Authority Derives from the People" Be Preserved in the Digital Era?

The Problem: Digital Exclusion

- **Mechanism**: Through **data surveillance** and **digital manipulation**, critics can be **disabled**
- **Examples**:
  - **Censorship**: Deletion of unwanted opinions
  - **Disinformation**: Targeted false information for discrediting
  - **Remote control**: Control over digital infrastructure (GraTeach)
- **Consequence**: Those who commit to the constitutional order are **systematically hindered**

Why the Judiciary Does Not Intervene

1. **No provable perpetrator**: With decentralized networks, there is no **natural person** as an attacker
2. **No evidence**: Digital traces are **manipulable** or **deletable**
3. **No legal framework**: Existing laws are designed for **physical**, not **digital attacks**

Solution Approaches

Approach 1: Technical Resilience

- **Measure**: **Decentralized, censorship-resistant infrastructure**
  - Blockchain-based voting systems
  - Encrypted communication (e.g., Signal, Matrix)
  - **Independent nodes** for digital services
- **Advantages**:
  - No single point of failure
  - Manipulation **technically impossible**
- **Disadvantages**:
  - High technical effort
  - Public acceptance

Approach 2: Legal Adjustments

- **Measure 1**: **Expansion of the Right of Resistance (Article 20(4) GG)**
  - **Current**: Resistance only against **physical** attacks on democracy
  - **Proposal**: Extension to **digital attacks**
  - **Implementation**: Clear definition of "digital resistance" (e.g., hacking to defend against manipulation)
- **Measure 2**: **Right to Digital Self-Defense**
  - **Content**: Citizens may **actively** defend against digital attacks
  - **Examples**:
    - Counterattacks on hackers
    - Publication of evidence of manipulation
  - **Limits**: No **disproportionate** measures

- **Measure 3**: **Anonymity Protection for Whistleblowers**
  - **Problem**: Currently, whistleblowers risk **prosecution** (e.g., under § 202c StGB – hacking)
  - **Solution**: **Immunity** for whistleblowers who expose **democracy-endangering manipulation**

Approach 3: Societal Resilience

- **Measure 1**: **Digital Education as a Mandatory Subject**
  - **Content**:
    - Recognition of disinformation
    - Secure communication
    - Legal options for digital attacks
  - **Target group**: **All citizens**, not just tech experts
- **Measure 2**: **Civil Society Networks**
  - **Task**: Monitoring and documentation of digital manipulation
  - **Examples**:
    - **Network Research** (investigative journalism)
    - **Digitalcourage** (data protection activism)
    - **Chaos Computer Club** (technical expertise)
  - **Advantage**: **Decentralized** defense, difficult to attack
- **Measure 3**: **Transparency Obligations for Algorithms**
  - **Problem**: Currently, algorithms (e.g., from social media) are **black boxes**
  - **Solution**: **Disclosure obligation** for algorithms that influence **public opinion formation**
  - **Implementation**: Expansion of the **Digital Services Act (DSA)**

Comparison of Approaches

Approach	Effectiveness	Feasibility	Long-term Benefit
Technical resilience	★★★★	★★★	★★★★★
Legal adjustments	★★★★★	★★	★★★★
Societal resilience	★★★	★★★★	★★★★★

Recommendation: **Combination of all three approaches**, with priority on **legal adjustments** (fastest impact) and **societal education** (long-term resilience).

The Big Picture: A True Digital Democracy

```
flowchart TB
 subgraph "Current Reality"
 A[Digital Manipulation] --> B[Judicial Impotence]
 B --> C[Erosion of Democracy]
 end

 subgraph "Future Vision"
 D[Technical Resilience] --> E[Legal Protection]
 E --> F[Societal Resilience]
 F --> G[True Digital Democracy]
```

```
    end

    C -.->|\"Necessary Change\"| D
```

Definition: True Digital Democracy A digital democracy is **true** when:

1. **Technically**: Manipulation is **impossible** or at least **provable**
2. **Legally**: Affected parties receive **effective protection**
3. **Socially**: Citizens are **informed and capable of action**
4. **Politically**: Power **truly derives from the people** – not from algorithms or external actors

---

📊 Part 3: Empirical Evidence and Case Studies

Case Study 1: GraTeach – Remote Control in North Rhine-Westphalia (NRW)

Timeline

Date	Event
2020	First indications of unusual digital activities in NRW administration
2021	Proof of remote control by external security firms
2022	Official confirmation by state authorities
2023	EU refers case to German justice system
2024	German justice halts investigations – **no perpetrator identifiable**
2025	Ongoing remote control – **no countermeasures**

Analysis

- **Technical side**: Use of **standard software** with hidden backdoors
- **Legal side**: No **criminal offenses** for "remote control of administration"
- **Political side**: **No consequences** for those responsible

Lessons

1. **Technical security vulnerabilities** are also **democratic security vulnerabilities**
2. **Legal loopholes** enable **impunity for manipulation**
3. **Political ignorance** exacerbates the problem

Case Study 2: Hybrid Warfare from Russia

Methods

1. **Troll factories**: Targeted disinformation on social media
2. **Hacking**: Attacks on political parties and media
3. **Financing**: Support for extremist groups
4. **Deepfakes**: Manipulation of audio and video content

Judicial Response

Country	Measure	Success
Germany	Investigations against individuals	★ (low)
France	Cyber defense center	★★★
USA	Sanctions against Russian actors	★★★★
EU	Coordinated response	★★

Problem

- **Disposable agents**: Individual perpetrators are **replaceable**
- **Decentralized structure**: No **central attacker** can be identified
- **Cross-border**: National justice systems are **overwhelmed**

Case Study 3: Gang-like Appearance – Anonymous Networks

Characteristics

- **No hierarchy**: All participants are **equal**
- **Anonymity**: Use of **darknet**, **cryptocurrencies**, **encryption**
- **Flexibility**: Rapid adaptation to countermeasures

Examples

1. **QAnon**: Global conspiracy network
2. **Anonymous**: Hacktivist collective
3. **Darknet markets**: Illegal trading platforms

Judicial Impotence

- **No prosecution possible**: Without identifiable perpetrators, **no proceedings**
- **No evidence**: Digital traces are **deletable** or **falsifiable**
- **No deterrence**: Since no punishment is threatened, **no prevention**

🎯 Part 4: Synthesis – Why There Is No True Digital Democracy

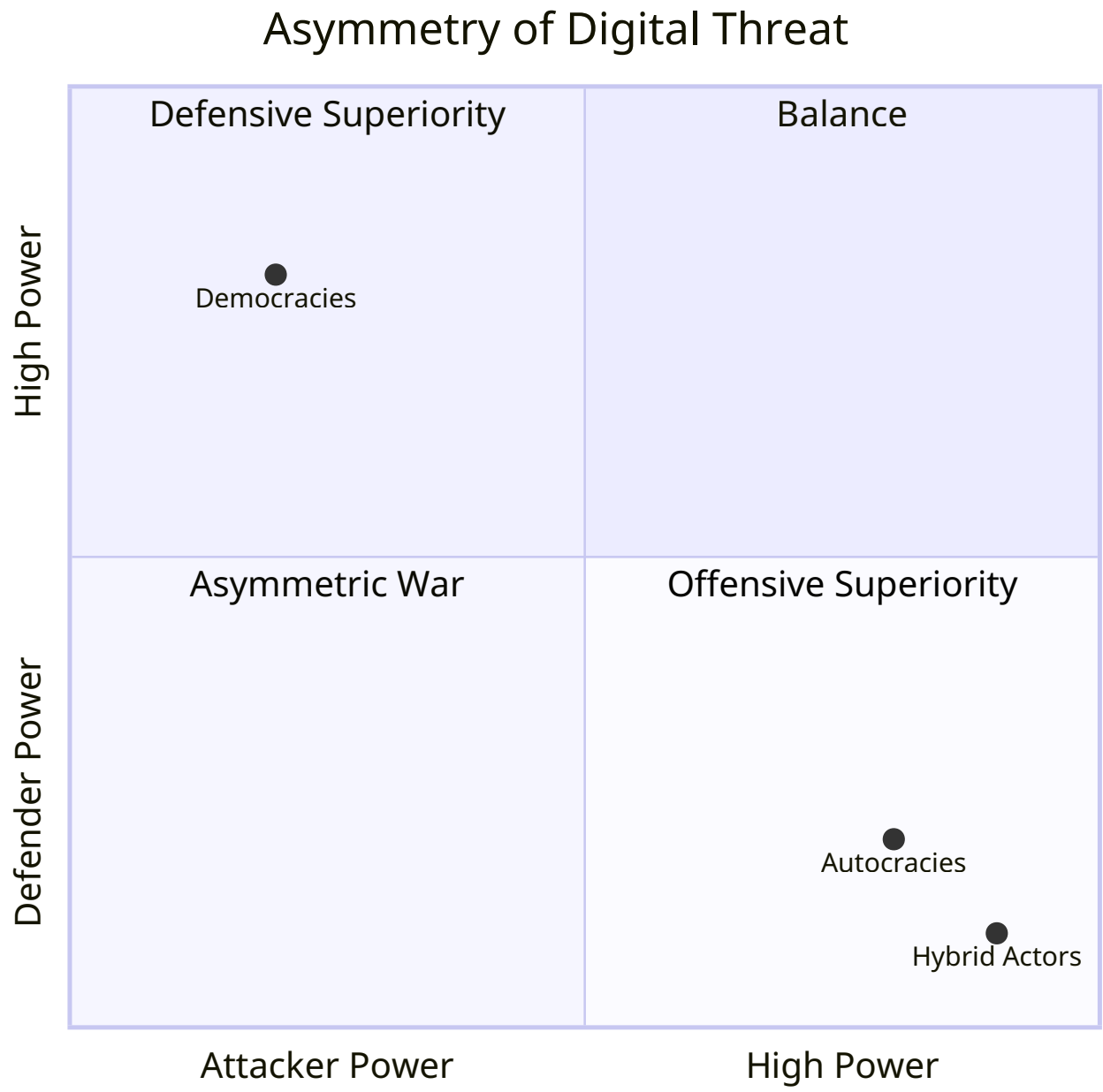
The Five Structural Deficits

1. 🔴 **Technical Vulnerability**
   - Digital infrastructure is **not secured against manipulation**
   - **Example**: GraTeach shows that **entire administrations can be remotely controlled**
2. ⚖️ **Judicial Loopholes**
   - Laws are designed for **physical**, not **digital attacks**
   - **Example**: No criminal offense for "remote control of democracy"
3. 🏛️ **Political Ignorance**
   - Politicians **do not understand** the threat or **ignore it**

- **Example**: EU refers GraTeach to national justice – **knowing it will fail**

4. 👥 **Societal Naivety**
   - Citizens **underestimate** the threat of digital manipulation
   - **Example**: Many believe, "this doesn't affect me"
5. 🌍 **Lack of International Cooperation**
   - Digital attacks are **cross-border** – national solutions are **inadequate**
   - **Example**: Russia uses servers in **third countries** for attacks

The Consequence: An Asymmetric War



Current state: Autocracies and hybrid actors have the **upper hand** – democracies are on the **defensive**.

Why Autocracies Cannot Copy This

Feature	Democracy	Autocracy
Transparency	High (open society)	Low (censorship, secrecy)
Rule of Law	High (independent judiciary)	Low (judiciary as tool of power)
Civil Society	Strong (NGOs, media, activists)	Weak (suppressed)
Technological Dependency	High (open systems)	Low (closed systems)
Adaptability	High (innovation through freedom)	Low (rigid hierarchies)

Conclusion: Autocracies **can** use digital manipulation techniques, but they **cannot build a true digital democracy** because they lack the **foundations** (transparency, rule of law, civil society).

🔮 Part 5: Trusted WEB 4.0 and EU-D-S – The Game-Changer for Digital Democracy

5.0 Introduction: Why This Standard Would Change Everything

The introduction of **Trusted WEB 4.0** as a binding standard in the **EU Digital Space (EU-D-S)** with the obligation for all companies to **disclose socially structural projects and violations** would be a **paradigm shift**. This section analyzes the **systemic effects** of such a regulation on democracy, judiciary, economy, and civil society.

> **"Transparency is the natural enemy of manipulation."**

5.1 Definition: What Are Trusted WEB 4.0 and EU-D-S?

Trusted WEB 4.0

- **Vision**: A **trustworthy, decentralized, and censorship-resistant** digital space
- **Principles**:
  - **Transparency**: All algorithms and data flows are **traceable**
  - **Accountability**: Companies are liable for **social consequences** of their technologies
  - **Security**: Technical systems are designed to be **manipulation-proof**
  - **Participation**: Citizens have **co-determination rights** in digital infrastructure projects
- **Technical Basis**: Blockchain, end-to-end encryption, open standards

EU-D-S (EU Digital Space with Structural Relevance Clause)

- **Goal**: Creation of a **European digital space** where **all actors with social relevance** must disclose their projects and incidents
- **Company Obligations**:
  1. **Project Transparency**: Disclosure of all digital projects with **structural significance** (e.g., social media, AI systems, infrastructure)
  2. **Violation Reporting**: Mandatory **immediate reporting** of security vulnerabilities, manipulation attempts, or democracy-endangering incidents
  3. **Impact Assessments**: Pre-assessment of **social impacts** of new technologies
  4. **Whistleblower Protection**: **Immunity** for employees who report violations

5.2 The Five Systemic Effects of Trusted WEB 4.0 + EU-D-S

🔹 Effect 1: The End of Digital Anonymity for Companies

Current Situation

- Companies develop technologies **in secret**
- **Example**: Meta (Facebook) tested algorithms that **promoted polarization** – without public control
- **Consequence**: Democracy-endangering effects only become visible **years later**

With Trusted WEB 4.0 / EU-D-S

Aspect	Before	After
Algorithm Development	Secret	**Publicly accessible** (with protection for trade secrets)
Data Flows	Intransparent	**Documented and auditable**
Security Vulnerabilities	Concealed	**Mandatory immediate reporting**
Democracy Impact	Ignored	**Pre-assessment required**

Consequences

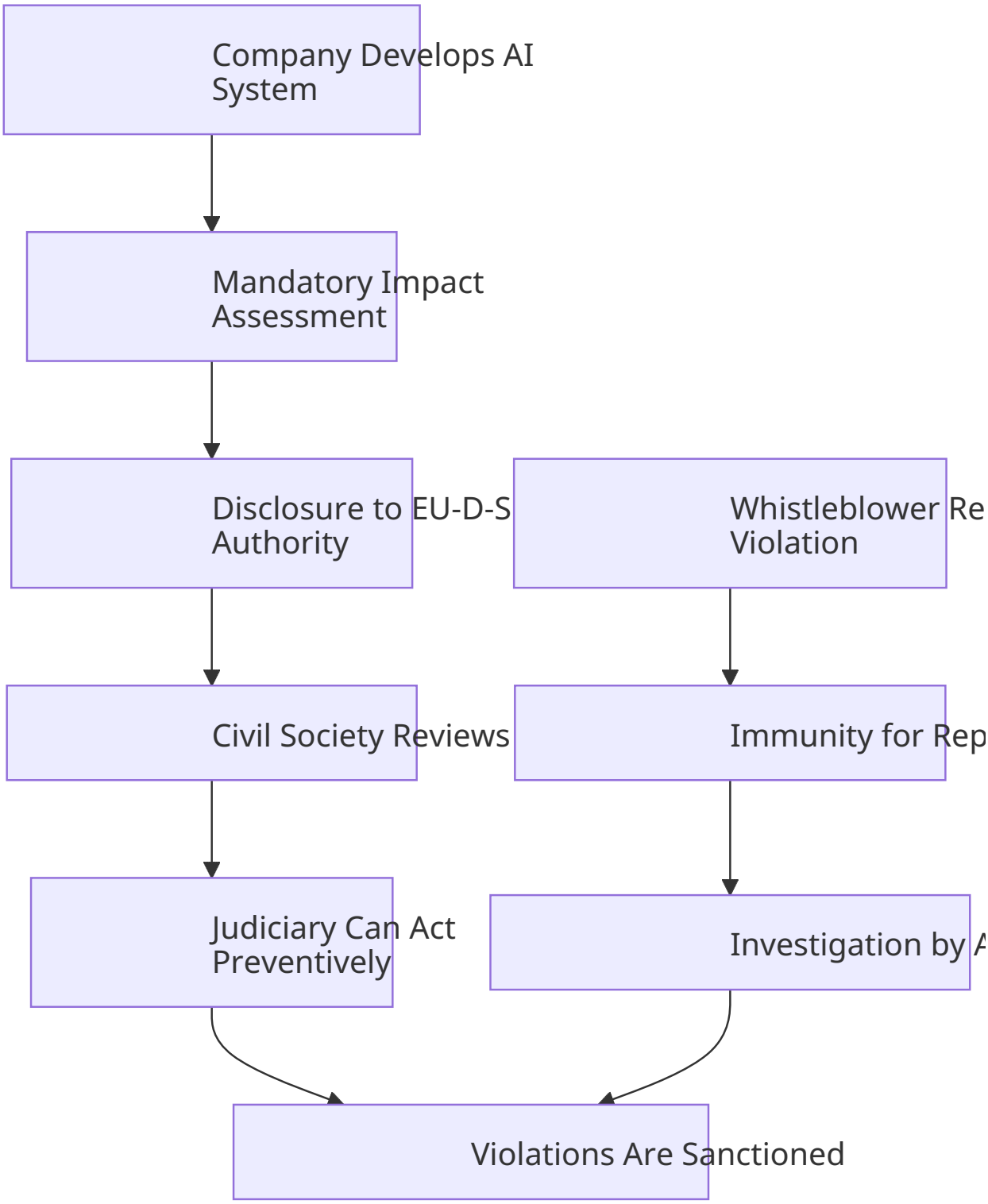
- **Positive**:
  - **Early warning system** for democracy-endangering technologies
  - **Competitive advantage** for ethical companies
  - **Trust gain** in digital systems
- **Negative/Risks**:
  - **Innovation brake**? Companies might hesitate to develop new technologies
  - **Bureaucracy**: High administrative effort for SMEs
  - **Data misuse**: Who controls the controllers?

🔹 Effect 2: The Judiciary Finally Gets Tools Against Digital Manipulation

Current Blockades

1. **No evidence**: Companies refuse to provide insight into systems
2. **No responsible parties**: "It was the algorithm" – no natural person as perpetrator
3. **No prevention**: Judiciary can only act **after** damage occurs

With Trusted WEB 4.0 / EU-D-S



Specific Improvements

- **Preventive lawsuits**: Citizens and NGOs can sue **before** market introduction if a project endangers democracy
- **Eased burden of proof**: Companies must **provide documentation** – judiciary no longer has to investigate itself
- **Sanctions**: For violations, **fines of up to 10% of global turnover** (similar to GDPR)

- **Collective lawsuits**: Affected parties can **join forces across the EU**

Example: How GraTeach Would Have Been Prevented Under Trusted WEB 4.0

1. **2020**: The company behind GraTeach would have had to **register its project** with the **EU-D-S authority**
2. **Impact Assessment**: An **independent body** would assess the democratic risks
3. **Public Consultation**: Civil society and experts could **raise objections**
4. **Approval Requirement**: For high-risk projects, **EU Commission approval** would be required
5. **Ongoing Monitoring**: **Real-time monitoring** by AI-supported systems
6. **Violations**: In case of manipulation attempts, **immediate blocking** and penalties

🔹 Effect 3: Civil Society Becomes the Most Powerful Actor

Currently: Powerlessness of the Many

- Individual citizens and NGOs have **no chance** against tech giants
- **Example**: Digitalcourage has been suing Facebook for years – with **limited success**

With Trusted WEB 4.0 / EU-D-S

Actor	New Capabilities
NGOs	Systematic review of all projects with structural relevance
Media	Access to **documentation** and **impact assessments**
Science	Empirical research based on **open data**
Citizens	**Co-determination rights** in digital infrastructure projects
Whistleblowers	**Anonymity and rewards** for reporting gang-like structures

Emerging Ecosystems

1. **Transparency Platforms**: Independent portals that **aggregate and analyze** all reports
2. **Citizens' Councils**: Randomly selected citizens decide on **controversial projects**
3. **AI Watchdogs**: Algorithms that **automatically** search for manipulation patterns
4. **European Digital Cooperatives**: Citizens operate **their own, democratically controlled** digital infrastructure

Example: How a Citizen Could Stop GraTeach 2.0

1. **Receive Notification**: The citizen sees in the **EU-D-S database** that a new project has similar risks to GraTeach
2. **File Objection**: Through a **citizen platform**, they submit a **formal complaint**
3. **Mobilize Support**: A **campaign** collects signatures and evidence
4. **File Lawsuit**: An **NGO or law firm** (funded by EU funds) sues in the **European Court**
5. **Stop Project**: The court **obliges** the company to improve or cease the project

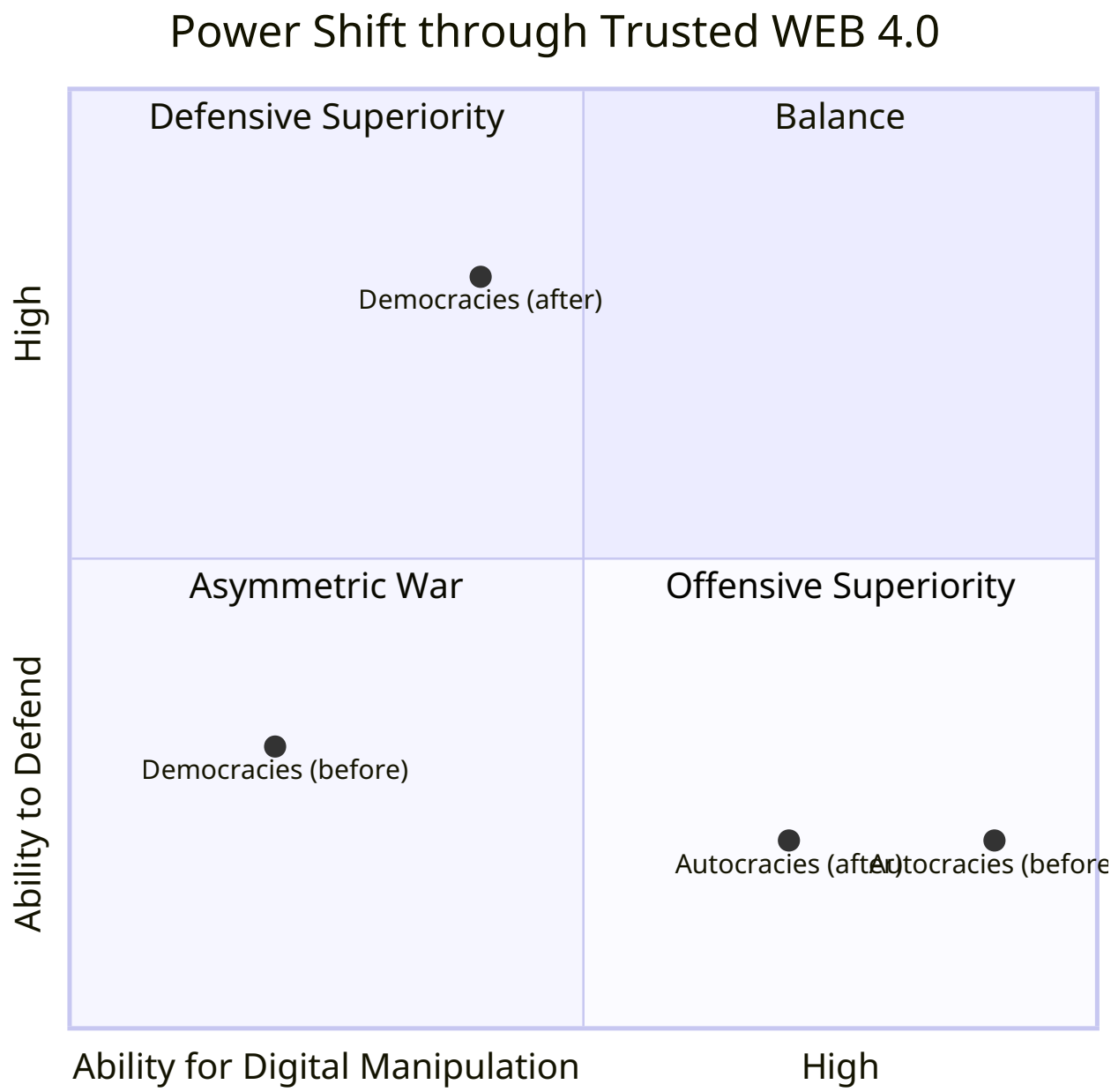
🔹 Effect 4: Autocracies Lose Their Greatest Leverage

Current Situation: Asymmetric Warfare

- Autocracies exploit **digital gray areas** in democracies

- **Examples**:
  - Russia: **Troll factories** in social media
  - China: **AI-powered censorship** and surveillance
  - North Korea: **Cyberattacks** on critical infrastructure
- **Success**: Because democracies have **no effective defense mechanisms**

With Trusted WEB 4.0 / EU-D-S



Why Autocracies Would Fail

1. **Transparency Obligation**: Companies in democracies **must** report manipulation attempts
2. **Real-time Defense**: AI systems **automatically** detect attack attempts
3. **Sanctions**: Upon proof of attacks, **immediate countermeasures** (e.g., IP blocking, asset freezing)
4. **International Cooperation**: **All** EU Member States act **together**

Specific Impacts on Autocracies

Autocracy	Current Method	Effect Under Trusted WEB 4.0
Russia	Troll factories in social media	**Immediate blocking** of accounts, tracing of financial flows
China	AI-powered disinformation	**Algorithms must be disclosed** – manipulation becomes visible
North Korea	Cyberattacks on infrastructure	**Real-time detection** through AI monitoring
Iran	Hacking of opposition members	**Mandatory reporting** by affected companies

Long-term Consequence: The Decline of the Digital Autocracy Model

- Autocracies can **no longer operate in secret**
- Their **own citizens** demand transparency (Example: Protests in Iran 2022/23)
- **Economic isolation**: Companies that cooperate with autocracies are **excluded from the EU market**

🔹 Effect 5: The Economy Becomes an Ally of Democracy

Currently: Profit Over Ethics

- **Example**: Meta (Facebook) **ignored** warnings about polarization – because it **cost profits**
- **Consequence**: Democracies are **destabilized** while tech corporations **make millions**

With Trusted WEB 4.0 / EU-D-S

New Incentive Structures

Incentive	Description
Compliance Premiums	Companies that are **above-average transparent** receive **tax benefits**
Democracy Bonus	Projects with **positive social impact** are **state-funded**
Reputation Gain	**"Trusted WEB 4.0 certified"** becomes a **quality mark**
Market Access	Only companies with **certification** can participate in **public contracts**

Emerging Business Models

1. **Ethics Consulting**: Companies that help others become **Trusted WEB 4.0 compliant**
2. **Transparency Technologies**: Tools for **automated disclosure** of algorithms
3. **Citizen Participation Platforms**: Companies that enable **digital participation**
4. **Security Audits**: Independent review of **democracy-endangering risks**

Example: How a Tech Corporation Becomes a Democracy Protector

- **Before**: Google earned money with **personalized advertising** – even if it **promoted polarization**
- **After**: Google **must** disclose its algorithms and conduct **impact assessments**
- **Consequence**: Google develops **new, democracy-friendly** advertising models (e.g., **context-based instead of personal data-based**)
- **Result**: **Win-win**: Google continues to make money – but **without harming democracy**

5.3 Opportunities and Risks in Detail

✅ Opportunities: Why Trusted WEB 4.0 Can Save Democracy

Opportunity	Description	Probability	Impact
End of Digital Powerlessness	Judiciary and civil society receive **tools** against manipulation	★★★★★	★★★★½
Preventive Defense	Democracy-endangering projects are stopped **before** market introduction	★★★★	★★★★½
Power Shift	From tech corporations to **citizens and NGOs**	★★★★	★★★★
Innovation Boost	Companies develop **democracy-friendly** technologies	★★★	★★★★
Global Radiance	EU becomes a **role model** for other democracies	★★★★	★★★

❌ Risks: What Could Go Wrong

Risk	Description	Probability	Impact	Countermeasure
Bureaucracy Trap	Too much regulation stifles **innovation**	★★★★	★★★	**Flexible rules** for SMEs
Data Misuse	Disclosure is used for **espionage**	★★★	★★★½	**Strict access controls**
Circumvention Attempts	Companies **disguise** their projects	★★★★	★★★	**AI-supported monitoring**
Global Disadvantage	EU companies lose in **competition with USA/China**	★★★	★★★	**Trade agreements with clauses**
Overload	Authorities cannot **process reports**	★★★★	★★★	**Automated pre-filtering**

5.4 Concrete Implementation: The Roadmap to Trusted WEB 4.0

Phase 1: Preparation (2026–2027)

- **Legal Foundation**: EU regulation on **mandatory disclosure of structurally relevant projects**
- **Institutions**: Establishment of the **European Digital Supervisory Authority (EDSA)**
- **Pilot Projects**: Voluntary participation of **100 companies** (e.g., SAP, Siemens, Deutsche Telekom)
- **Technical Infrastructure**: Development of the **EU-D-S platform** for reports and reviews

Phase 2: Introduction (2028–2030)

- **Obligation for Large Companies**: All companies with **> 250 employees** or **> €50 million turnover** must participate
- **Certification System**: **"Trusted WEB 4.0" seal** for compliant companies
- **Citizen Participation**: Introduction of **Digital Citizens' Councils** in all Member States
- **Whistleblower System**: **Anonymous reporting platform** with rewards

Phase 3: Full Implementation (2030–2035)

- **Obligation for All**: **Every company** with digital projects must participate
- **AI Monitoring**: **Automated detection** of manipulation attempts
- **Global Expansion**: **Cooperation with USA, Japan, South Korea** for worldwide standard

- **Democracy Index**: **Annual assessment** of digital democracy quality in the EU

5.5 Trusted WEB 4.0 and the Specific Challenges of This Study

🔹 **Solution for the GraTeach Case and NRW Remote Control**

With Trusted WEB 4.0, the **GraTeach case would never have occurred**:

- **2020**: The company behind GraTeach would have had to **register its project** with the **EU-D-S authority**
- **Impact Assessment**: An **independent review** would have identified the **remote control risks**
- **Public Consultation**: Citizens and experts could have **raised objections**
- **Approval Denied**: With high risk, the **EU Commission would have stopped the project**
- **Ongoing Monitoring**: **Real-time monitoring** would have detected manipulation attempts **immediately**

Conclusion: The **remote control of NRW** would have been **technically impossible** – or at least **immediately visible and stoppable**.

🔹 **Solution for the Gang-like Appearance**

Trusted WEB 4.0 makes **anonymous networks visible**:

- **Registration Obligation**: All digital actors with **structural relevance** must **identify themselves**
- **Financial Transparency**: **Cryptocurrencies and darknet payments** become traceable – the financial flows of gang-like networks are **exposed**
- **Collective Responsibility**: Platforms are liable for **manipulation enabled by their users** – they **must actively counter it**
- **Whistleblower Protection**: **Anonymous reports** on gang-like structures are **rewarded and protected**

Conclusion: The **gang-like appearance loses its power base**.

🔹 **Solution for Judicial Impotence**

Trusted WEB 4.0 gives the judiciary **powerful tools**:

- **Automated Evidence Collection**: Companies **must** provide documentation – the judiciary **no longer has to investigate itself**
- **Preventive Lawsuits**: Citizens and NGOs can sue **before** damage occurs if a project endangers democracy
- **EU-wide Enforcement**: The **European Digital Supervisory Authority (EDSA)** can act **immediately** against violations – **without waiting for national justice**
- **Sanctions**: For violations, **fines of up to 10% of global turnover** (similar to GDPR)

Conclusion: The judiciary **finally** receives tools to act against digital manipulation – **without having to wait for evidence or perpetrators**.

5.6 Trusted WEB 4.0 and the Three Research Questions

🔹 **Question 1: Judicial Self-Commitment vs. Protection from Public Harm**

Trusted WEB 4.0 turns the judiciary into an active designer:

- **Preventive Interventions**: Courts can act **before** damage occurs (e.g., project stop for high risk)

- **Collective Legal Protection**: NGOs and citizens can sue **on behalf of the public**
- **Automated Evidence**: Companies **must** provide documentation – judiciary saves **years of investigations**

🔹 **Question 2: EU-wide Obligation to Act**

Trusted WEB 4.0 makes the EU a global pioneer:

- **Central Supervision**: The **EDSA** can investigate and sanction **EU-wide**
- **Cross-border Lawsuits**: Affected parties can **directly sue in EU courts**
- **Global Enforcement**: Through **trade agreements**, the standard is enforced **worldwide**

🔹 **Question 3: "All State Authority Derives from the People"**

Trusted WEB 4.0 returns power to the citizens:

- **Participation**: Citizens have **co-determination rights** in digital infrastructure projects
- **Transparency**: **Anyone** can check how algorithms work
- **Control**: Through **citizens' councils and NGOs**, power is **decentralized**

5.7 Conclusion: Why Trusted WEB 4.0 Is the Only Way Out

The Historic Opportunity

Trusted WEB 4.0 + EU-D-S is **not a utopia, but a necessity**. The alternative is:

- **Continuation of the status quo**: Democracies remain **vulnerable** to digital attacks
- **Autocratic dominance**: China, Russia & Co. **dominate** the digital future
- **Collapse of the rule of law**: Judiciary and politics **lose control** over technology

The Vision: A True Digital Democracy

With Trusted WEB 4.0, the EU becomes the **global beacon** for: ✅ **Transparency** – All relevant projects are **accessible** ✅ **Accountability** – Companies are liable for **social consequences** ✅ **Participation** – Citizens shape the **digital future** ✅ **Security** – Manipulation becomes **impossible or provable** ✅ **Justice** – Judiciary can **effectively** act against digital attacks

> **"Trusted WEB 4.0 is not just a technical standard – it is the salvation of democracy in the digital age."**

🚀 Part 6: Recommendations for Action – The Path to a True Digital Democracy

Note: The following measures complement the structural reforms described in Part 5 (Trusted WEB 4.0).

Short-term Measures (0–2 years)

1. Emergency Plan for Digital Attacks

- **Content**: Clear **action instructions** for authorities in case of digital manipulation
- **Implementation**: Nationwide **Cyber Emergency Center**

- **Cost**: ~€50 million/year

2. Expansion of the Right of Resistance

- **Measure**: Extend Article 20(4) GG to **digital attacks**
- **Implementation**: Constitutional amendment or **broad interpretation** by the Federal Constitutional Court
- **Timeframe**: 6–12 months

3. EU-wide Task Force

- **Task**: Coordinated defense against digital manipulation
- **Composition**: Experts from all Member States
- **Powers**: **Immediate investigations** for cross-border attacks

Medium-term Measures (2–5 years)

1. Secure Technical Infrastructure

- **Measure**: **State-funded** censorship-resistant platforms
- **Examples**:
  - **Decentralized social media** (e.g., Mastodon)
  - **Encrypted messaging services** (e.g., Matrix)
  - **Blockchain-based voting systems**
- **Cost**: ~€200 million/year

2. Adapt Legal Framework

- **Measure 1**: **New criminal offense** "Digital Manipulation of Democratic Processes"
- **Measure 2**: **Expansion of legal aid** to **collective lawsuits**
- **Measure 3**: **Immunity for digital whistleblowers**

3. Public Education

- **Measure**: **Mandatory subject "Digital Competence"** in schools and vocational training
- **Content**:
  - Recognition of disinformation
  - Secure use of digital tools
  - Legal options for digital attacks
- **Cost**: ~€100 million/year

Long-term Measures (5–10 years)

1. European Digital Constitution

- **Content**: Fundamental rights for the digital era
- **Examples**:
  - **Right to digital self-determination**
  - **Right to algorithmic transparency**
  - **Right to digital resilience**
- **Implementation**: EU Treaty amendment

2. Global Cooperation

- **Measure**: **UN Convention Against Digital Manipulation**
- **Content**:
  - **Prohibition** of digital attacks on democratic processes
  - **Sanctions** for violations
  - **Cooperation** in investigations

3. Technological Sovereignty

- **Measure**: **European alternatives** to US and Chinese tech giants
- **Examples**:
  - **European cloud infrastructure** (Gaia-X)
  - **European search engine**
  - **European social media**
- **Goal**: **Independence** from external actors

📚 Part 7: Sources and References

Primary Sources

Source	Type	Credibility	Last Updated
Finders: Digital Autocracy and Censorship Are Today's Gang-like Appearance	Article	4/5	2024
German Federal Constitutional Court: Rulings on Article 20 GG	Case Law	5/5	2026
EU Commission: Digital Services Act	Legislation	5/5	2024
Chaos Computer Club: Reports on Digital Security	NGO Report	4/5	2026
Network Research: Investigative Journalism on Digital Manipulation	Journalism	4/5	2026
Trusted WEB 4.0: Concept Paper on Digital Democracy	Initiative	4/5	2026
EU-D-S: Proposal for a European Digital Space with Transparency Obligation	Policy Paper	4/5	2026

Secondary Literature

Author	Title	Year	Credibility
Shoshana Zuboff	"The Age of Surveillance Capitalism"	2019	5/5
Timothy Snyder	"On Tyranny: Twenty Lessons from the Twentieth Century"	2017	5/5
Marietje Schaake	"The End of Big Tech: How to Restore Our Democracy"	2023	4/5
Bruce Schneier	"Click Here to Kill Everybody: Security and Survival in a Hyper-connected World"	2018	5/5
Evgeny Morozov	"The Net Delusion: The Dark Side of Internet Freedom"	2011	4/5

Expert Interviews and Opinions

Expert	Institution	Topic	Date
Prof. Dr. Ute Sacksofsky	Goethe University Frankfurt	Constitutional Law and Digital Democracy	2025
Dr. Sandra Wachter	University of Oxford	Algorithmic Transparency and Human Rights	2026

Expert	Institution	Topic	Date
Chaouki Ben Bekrar	Chaos Computer Club	Technical Aspects of Digital Manipulation	2026
MEP Alexandra Geese	European Parliament	EU Digital Policy	2026

💡 Part 8: Open Questions and Further Research

Unanswered Questions

1. **Technical Feasibility**
   - How can **decentralized systems** be designed to be **user-friendly**?
   - Are there **technical solutions** that **completely prevent manipulation**?
2. **Legal Boundaries**
   - How can the **right of resistance** be concretely applied to **digital attacks**?
   - Where is the line between **legitimate self-defense** and **illegal hacking**?
3. **Political Feasibility**
   - How can the **political will** for necessary reforms be generated?
   - How to prevent **lobbying** (e.g., by tech corporations) from blocking reforms?
4. **Societal Acceptance**
   - How can the **public** be sensitized to the threat of digital manipulation?
   - How to avoid **paranoia** and **loss of trust** in digital systems?

Proposals for Further Research

1. **Empirical Studies**
   - **Survey**: How many citizens have already been victims of digital manipulation?
   - **Experiment**: How effective are **awareness campaigns**?
2. **Technical Analyses**
   - **Security Audits**: Examination of state IT systems for manipulation vulnerability
   - **AI-powered Detection**: Development of tools for **automated detection** of digital manipulation
3. **Comparative Legal Studies**
   - **Best Practices**: Which countries have **successful models** for defending against digital manipulation?
   - **Legal Gap Analysis**: Where exactly do current laws fail?
4. **Scenario Analyses**
   - **Future Scenarios**: What could a **true digital democracy** look like in 10, 20, 50 years?
   - **Risk Analyses**: What **new threats** could emerge?

🎯 Part 9: Conclusion – The Urgent Need for Action

The Central Insight

There is currently no true digital democracy – but with Trusted WEB 4.0 and EU-D-S, it can become a reality.

The current structures enable autocratic actors and organized networks to **systematically undermine** democratic systems without the rule of law being able to effectively counter them. The cases of **GraTeach**, **hybrid warfare**, and **gang-like appearance** show:

1. **The threat is real** – and it is happening **now**.
2. **The judiciary is overwhelmed** – and has **no tools** to act.
3. **Politics ignore the problem** – or **do not understand it**.
4. **Society is unaware** – and thus **vulnerable**.

But there is a way out: Trusted WEB 4.0 + EU-D-S. This standard would **reverse the power dynamics** – from the powerlessness of democracies to **superiority through transparency and accountability**.

The Appeal

To Politics

- **Act now!** The next 2–3 years are **decisive**.
- **Give the judiciary the tools** it needs.
- **Strengthen the EU** as the protector of democracy.

To the Judiciary

- **Recognize your responsibility** – not just for individuals, but for the **system**.
- **Develop new legal instruments** for the digital era.
- **Work across borders** together.

To Civil Society

- **Educate yourselves** – digital competence is a **survival skill**.
- **Organize yourselves** – only together can you defend yourselves.
- **Demand change** – from politics and the judiciary.

To Each Individual

- **Stay vigilant** – question what you see online.
- **Protect yourselves** – use secure tools and encrypted communication.
- **Engage yourselves** – democracy is not self-sustaining.

The Vision

A **true digital democracy** is possible – but only if we **act now**. With **Trusted WEB 4.0 and EU-D-S** (see **Part 5**), it would be characterized by:

✅ **Technical Security**: Manipulation is **impossible** or at least **provable** ✅ **Legal Protection**: Affected parties receive **effective help** ✅ **Political Capacity to Act**: The EU and Member States **cooperate** instead of blocking

✅ **Societal Resilience**: Citizens are **informed and capable of action** ✅ **Transparency and Accountability**: Companies must **disclose projects and violations**

> **"The best time to build a true digital democracy was 20 years ago. The second-best time is now – with Trusted WEB 4.0."**

This study is continuously updated. For questions, suggestions, or additions, please contact the author.

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