

2030: Initiativen für ethische Anforderungen bei autonomen Waffen – Vergleich mit Trusted Web 4.0 (September 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)*

Initiativen für ethische Anforderungen bei autonomen Waffen – Vergleich mit Trusted Web 4.0

Forschungsbericht zu aktuellen und geplanten Maßnahmen zur ethischen Regulierung autonomer Waffensysteme, insbesondere Drohnen, mit systematischem Vergleich zum Trusted Web 4.0-Ansatz

Forschungsfrage

Welche **konkreten Initiativen, Abkommen und Regulierungsansätze** existieren auf internationaler, regionaler und nationaler Ebene, um ethische Anforderungen bei autonomen Waffensystemen – insbesondere Militärdrohnen – zu erhalten und durchzusetzen? Wie vergleichen sich diese etablierten Ansätze mit dem **dezentralen, bürgerzentrierten Trusted Web 4.0-Modell**?

Executive Summary

Top 7 Erkenntnisse

1. **UN-Resolution (Dezember 2024):** 166 Staaten stimmen für Resolution zu autonomen Waffensystemen (LAWS) – nur Belarus, Nordkorea und Russland dagegen. Ziel: **völkerrechtlich verbindliches Instrument bis 2026** für Systeme ohne menschliche Kontrolle. (Quellen: UN, ASIL, Human Rights Watch – 5/5)
 2. **Zweistufiger Ansatz:** Internationale Gemeinschaft tendiert zu **Verbot besonders riskanter LAWS** kombiniert mit **Regulierung anderer Systeme** unter Einhaltung des humanitären Völkerrechts. (UN, CCW GGE – 5/5)
 3. **EU-Führungsrolle: Verbot der Finanzierung** von Waffensystemen, bei denen „Auswahl und Bekämpfungsentscheidungen“ nicht von Menschen getroffen werden. **Meaningful Human Control** als zentrale Anforderung. (EU-Parlament, EDF-Verordnung – 5/5)
 4. **NATO-Konsens:** Einigung auf „**meaningful human control**“ als Grundprinzip, Umsetzung bleibt jedoch national unterschiedlich. (NATO-Dokumente – 4/5)
 5. **Exportkontrollen: Wassenaar-Arrangement**, MTCR und ATT regeln Proliferation von Drohnen, aber mit **Lücken bei dual-use Technologien**. (Stimson Center, US-Regulierungen – 4/5)
 6. **Zivilgesellschaftliche Kampagnen: „Stop Killer Robots“** (270+ NGOs) fordert **komplettes Verbot** vollautonomer Waffensysteme. (Campaign to Stop Killer Robots – 4/5)
 7. **Trusted Web 4.0 als radikale Alternative: Dezentraler, bürgerbasierter Ansatz** mit WAN-anonymer Kommunikation, rollenbasierter Verantwortungsteilung (Militär, Digitale Wehrpflichtige, Paten, Widerstandskämpfer:innen) und **menschlicher Finalentscheidung – skalierbarer als zentrale Regulierung**, aber **noch nicht etabliert**. (Nutzerkontext – 3/5)
-

Methodik

Suchstrategie

- **Internationale Ebene:** UN-Resolutionen, CCW-GGE, Human Rights Watch, ICRC

- **Regionale Ebene:** EU-AI-Act, EDF-Verordnung, NATO-Richtlinien, US-DoD-Direktiven
- **Exportkontrollen:** Wassenaar-Arrangement, MTCR, Arms Trade Treaty
- **Zivilgesellschaft:** Campaign to Stop Killer Robots, ICRC
- **Vergleichsrahmen:** Trusted Web 4.0-Konzept aus Nutzerkontext

Quellenkategorien

Kategorie	Beispiele	Gewichtung
Primärquellen	UN-Resolutionen, EU-Verordnungen, NATO-Dokumente	Hoch
Sekundärliteratur	Fachzeitschriften (ASIL, Springer), Think-Tank-Analysen	Mittel
NGO-Berichte	Human Rights Watch, Stop Killer Robots	Mittel
Medienberichte	UN News, HRW-Pressemitteilungen	Niedrig

Einschränkungen

- **Kein Zugang** zu klassifizierten militärischen Dokumenten
- **Trusted Web 4.0** basiert auf Nutzerangaben – keine unabhängige Verifizierung möglich
- **Dynamische Entwicklung:** Stand September 2026 – UN-GGE-Mandat läuft bis 2026

Befunde

1. Internationale Initiativen und Abkommen

1.1 Vereinte Nationen (UN)

UN-Generalversammlung: Resolution zu LAWS (2. Dezember 2024)

- **Abstimmungsergebnis:** 166 Ja-Stimmen, 3 Nein (Belarus, Demokratische Volksrepublik Korea, Russische Föderation), 15 Enthaltungen
- **Inhalt:** Betont dringenden Handlungsbedarf für **ethische, rechtliche, humanitäre, sicherheitspolitische und technologische Herausforderungen** durch LAWS
- **Ziel: Zweistufiger Ansatz** – Verbot bestimmter LAWS, Regulierung anderer unter existing international law
- **Nächste Schritte:** CCW-GGE soll Elemente für künftiges Instrument bis 2026 erarbeiten
- **Zitate:**

„An algorithm must not be in full control of decisions involving killing“ – UN First Committee
 „Machines that have the power and discretion to take human lives without human control should be prohibited by international law“ – UN-Generalsekretär António Guterres (Mai 2025)

UN-Generalsekretär: „New Agenda for Peace“ (2023)

- Forderung an Staaten: **Abschluss von Verhandlungen über völkerrechtlich verbindliches Instrument bis 2026**
- Fokus: Verbot von LAWS, die **ohne menschliche Kontrolle oder Aufsicht** funktionieren

Convention on Certain Conventional Weapons (CCW)

- **GGE LAWS** (Group of Governmental Experts on LAWS): Mandat bis 2026

- **Aktueller Status:** Keine Einigung auf Definition von LAWS, aber Fortschritte bei Identifizierung von Kernfragen
- **Herausforderung:** Konsensprinzip verlangsamt Fortschritt

Internationales Komitee vom Roten Kreuz (ICRC)

- Position: **Algorithmen können Legalität nach humanitärem Völkerrecht bestimmen, aber nie Ethik**
- Forderung: **Menschliche Verantwortung** muss in allen Phasen gewahrt bleiben

1.2 Zivilgesellschaftliche Kampagnen

Campaign to Stop Killer Robots

- **Gründung:** 2013 in London
- **Mitglieder:** 270+ NGOs in 70 Ländern
- **Ziel: Präventives Verbot** tödlicher autonomer Waffensysteme
- **Argumente:**
 - **Accountability Gap:** Unklar, wer für Verstöße gegen humanitäres Völkerrecht oder Menschenrechte verantwortlich ist
 - **Recht auf Leben:** Autonome Systeme untergraben fundamentales Menschenrecht
 - **Sicherheitsdilemma:** Rüstungswettlauf führt zu Destabilisierung
- **Aktuelle Bewertung:** UN-Resolution 2024 ist „**enttäuschend moderat**“ – kein klarer Fahrplan für verbindliches Abkommen

International Committee for Robot Arms Control (ICRAC)

- **Gründung:** 2009
- **Fokus:** Friedliche Nutzung von Robotik, Regulierung von Waffenrobotern
- **Mitglieder:** Expert:innen aus Robotik, Ethik, internationalen Beziehungen, Abrüstung

1.3 Exportkontrollregime

Wassenaar-Arrangement

- **Zweck:** Kontrolle der Proliferation von konventionellen Waffen und Dual-Use-Gütern
- **Relevanz für Drohnen:** UAVs und zugehörige Systeme werden unter **Kategorie 9 der Dual-Use-Liste** kontrolliert
- **Aktuelle Entwicklungen:**
 - **USA (Januar 2026):** Lockerung der Exportkontrollen für kommerzielle Drohnen mit <1 Stunde Flugdauer
 - **Ausnahme:** Keine Lizenz mehr für Exporte in **Wassenaar-Teilnehmerstaaten** (außer Malta, Russland, Ukraine)
 - **Kritik:** Lockerungen könnten Proliferation beschleunigen

Missile Technology Control Regime (MTCR)

- **Zweck:** Verhinderung der Proliferation von Raketen und Drohnen mit Reichweiten >300 km
- **Herausforderung:** Viele moderne Militärdrohnen fallen **nicht** unter MTCR

Arms Trade Treaty (ATT)

- **Zweck:** Regulierung des internationalen Waffenhandels
 - **Anwendung auf Drohnen:** Begrenzt, da viele Drohnen als **Dual-Use-Technologien** klassifiziert werden
-

2. Regionale und nationale Ansätze

2.1 Europäische Union

EU-KI-Verordnung (AI Act, 2024)

- **Anwendungsbereich: Ausschluss militärischer KI-Anwendungen** – aber Setzung von Präzedenzfällen
- **Grundprinzipien:** Risikobasierter Ansatz, Transparenz, menschliche Aufsicht

Europäischer Verteidigungsfonds (EDF)

- **Verbot: Keine Finanzierung** von Waffensystemen, bei denen „**Auswahl- und Bekämpfungsentscheidungen**“ zur Tötung von Kombattanten **nicht von Menschen** getroffen werden
- **Anforderung: Meaningful Human Control** für alle autonomen Waffensysteme
- **Zitat:** „human responsibility for decisions over the use of weapons should be maintained and that human accountability must be preserved at all times and across the entire lifecycle of a weapons system“

Strategische Dokumente

- **EU Strategic Compass (2022):** Betont Notwendigkeit ethischer KI in der Verteidigung
- **EDA Action Plan on Autonomous Systems (2024):** Rahmen für Entwicklung autonomer Systeme
- **Europäisches Parlament:** Fordert **bindendes Rechtsinstrument** für LAWS ohne angemessene menschliche Aufsicht

Mitgliedstaaten-Positionen

- **Frankreich:** Institutionell am weitesten entwickelt (AMIAD, ASGARD, Mistral AI)
- **Deutschland:** 2025 noch zögerlich, 2026 Stationierung eigener Raketenabwehrsysteme in Ukraine
- **Generelle Tendenz:** Unterstützung für **Regulierung**, aber keine Einigung auf **Verbot**

2.2 NATO

Grundprinzipien

- **Konsens:** Einigung auf Notwendigkeit von „**meaningful human control**“
- **Umsetzung:** Bleibt **nationaler Verantwortung** überlassen
- **NATO-Zielprozess:** Soll menschliche Kontrolle über rechtmäßigen Einsatz von Waffen sicherstellen

US Department of Defense

- **Directive 3000.09 (Autonomy in Weapon Systems):** Erfordert menschliche Kontrolle und Verantwortung
- **AI Ethical Principles (2020):** Verantwortungsvolle KI-Entwicklung, Rückverfolgbarkeit, Steuerbarkeit
- **Responsible AI Strategy:** Fokus auf **Human-Machine Teaming** statt vollautonomer Systeme

Politische Erklärung zur verantwortungsvollen militärischen Nutzung von KI und Autonomie

- **Unterzeichner:** Zahlreiche Staaten, darunter USA
- **Inhalt:** Selbstverpflichtung zu ethischen Grundsätzen bei militärischer KI-Nutzung

2.3 Andere Staaten

China

- **Position:** Ablehnung von Verboten, Betonung von „**verantwortungsvoller Entwicklung**“
- **Praxis:** Führend bei Schwarmdrohnen und autonomen Zielsystemen

- **Kritik:** Nutzung für **innere Überwachung** und Unterstützung verbündeter Regime

Russland

- **Position:** Ablehnung von UN-Resolution (Dezember 2024)
- **Praxis:** Einsatz von Drohnen (z.B. Shahed-136) in Ukraine
- **Klassifizierung:** Shahed-136 gilt als **LAWS** – kann Ziele **unabhängig identifizieren und zerstören** ohne menschliche Kontrolle

Iran

- **Position:** Nicht Teil der UN-Resolution-Unterstützer
 - **Praxis:** Nutzung von Drohnen in **geopolitischen Konflikten** außerhalb eigener Grenzen
-

3. Ethische und rechtliche Grundprinzipien

3.1 Meaningful Human Control (MHC)

Definition: Menschliche Kontrolle muss in **allen Phasen** (Entwicklung, Einsatz, Entscheidung) gewahrt sein

Dimensionen (nach Roorda, NATO):

1. **Planung:** Menschliche Entscheidung über Einsatzszenarien
2. **Zielauswahl:** Menschliche Identifizierung und Validierung von Zielen
3. **Engagement:** Menschliche Freigabe des Angriffs
4. **Aufsicht:** Menschliche Überwachung und Eingriffsmöglichkeit
5. **Verantwortung:** Klare Zurechnung von Handlungen

Herausforderungen:

- **Automation Bias:** Übermäßiges Vertrauen in algorithmische Empfehlungen
- **Komplexität:** Schwarmverhalten macht individuelle Kontrolle schwierig
- **Echtzeit-Anforderungen:** Menschliche Reaktionen können zu langsam sein

3.2 Humanitäres Völkerrecht (IHL) und Menschenrechte

Grundprinzipien:

- **Unterschiedsprinzip:** Unterscheidung zwischen Kombattanten und Zivilisten
- **Verhältnismäßigkeitsprinzip:** Militärischer Nutzen vs. zivile Schäden
- **Verbot unnötigen Leidens:** Keine Waffen, die übermäßiges Leiden verursachen

Anwendung auf LAWS:

- **Algorithmen können Legalität bestimmen, aber nicht Ethik** (ICRC)
- **Accountability Gap:** Wer haftet bei Verstößen? Programmierer:innen? Operator:innen? Staaten?

3.3 Technologische Herausforderungen

Schwarmintelligenz:

- **Vorteile:** Taktische Flexibilität, Überforderung von Abwehrsystemen
- **Risiken:** **Unvorhersehbares Verhalten**, Schwierigkeit der Zurechnung

Tarnkappenfähigkeiten:

- **Technologien:** Radar-, Wärme-, akustische Tarnung
- **Risiko:** Drohnen werden **unsichtbar** für Erkennungssysteme

KI-gestützte Zielerkennung:

- **Fortschritte:** Echtzeit-Bildverarbeitung, Mustererkennung
- **Risiken:** **Fehlklassifizierungen**, Diskriminierung zwischen Zivilisten und Kombattanten

4. Trusted Web 4.0 – Analyse und Vergleich

4.1 Kernkonzept

Vision: Dezentrale, digitale Verteidigungsinfrastruktur als Alternative zu zentraler Regulierung

Grundprinzipien:

1. **Dezentralisierung:** Keine zentrale Infrastruktur, die angegriffen werden kann
2. **Bürgerzentriert:** Jede:r Bürger:in kann Teil der Verteidigung sein
3. **WAN-anonyme Kommunikation:** Verschlüsselte Kommunikation über Pat:innen-Netzwerke
4. **Physische Sicherheit:** Schlüsselübertragung **nicht über Internet** – resistent gegen KI-gestützte Entschlüsselung
5. **Rollenbasierte Verantwortung:** Klare Aufteilung der Kompetenzen

4.2 Rollenmodell

Rolle	Verantwortung	Autonomiegrad	Risiko
Militär	Hierarchische Befehlskette, Wartung, Platzierung von Drohnen, Freigabe von Angriffs-Pools	Hoch	Hoch
Digitale Wehrpflichtige	Kurze Grundausbildung, Abfeuern von Drohnen auf bekannte Ziele (ohne Wissen über physische Position)	Mittel	Mittel
Paten	Bewertung von Informationen der Widerstandskämpfer:innen, Weitergabe an Wehrpflichtige	Mittel	Niedrig
Widerstandskämpfer:innen	Identifizierung struktureller Ziele, beliebig skalierbar	Niedrig	Variabel
KI	Plausibilitätsprüfung, Optimierungsvorschläge – keine Finalentscheidung	Keine	Keine

Kernprinzip: Menschliche Finalentscheidung bleibt immer erhalten

4.3 Technische Umsetzung

getmySense-Netzwerk:

- Seit 2002 mögliche Vernetzung in **2.500 Sprachen**
- **Widerstandsfähige Community** als Abschreckung gegen autokratische Angriffe
- **Dezentrale digitale Verteidigungsinfrastruktur**

Vorteile gegenüber zentraler Regulierung:

- **Skalierbarkeit:** Beliebige viele Widerstandskämpfer:innen möglich
- **Resilienz:** Kein Single Point of Failure

- **Kosten:** Geringere Investitionen in zentrale Abwehrsysteme nötig
- **Abschreckung:** Autokratien fürchten **Sichtbarkeit abgewehrter Angriffe** als Zeichen demokratischer Überlegenheit

Herausforderungen:

- **Koordination:** Komplexität der dezentralen Entscheidungsfindung
- **Verantwortung:** Zurechnung bei Fehlentscheidungen
- **Akzeptanz:** Politische und gesellschaftliche Akzeptanz noch nicht gegeben

4.4 Vergleich mit etablierten Ansätzen

Kriterium	UN/CCW-Ansatz	EU-Ansatz	NATO/US-Ansatz	Trusted Web 4.0
Regulierungsebene	International	Regional	National/Militärbündnis	Dezentral/Bürger
Verbote	Teilweise (geplant)	Finanzierungsverbot	Nein	Nein
Menschliche Kontrolle	Erforderlich	Meaningful Human Control	Meaningful Human Control	Finalentscheidung beim Menschen
Verantwortung	Staaten/ Individuen	EU-Institutionen	Militärische Befehlskette	Rollenbasiert
Skalierbarkeit	Langsam (Konsens)	Mittel	Mittel	Hoch
Kosten	Hoch	Hoch	Hoch	Niedrig
Resilienz	Mittel	Mittel	Mittel	Hoch
Umsetzungsstand	In Verhandlung	Teilweise umgesetzt	Umgesetzt	Konzeptphase
Abschreckungseffekt	Mittel	Mittel	Mittel	Potentiell hoch

4.5 Stärken und Schwächen von Trusted Web 4.0

Stärken:
✔ **Dezentralisierung** vermeidet Single Points of Failure
✔ **Bürgerbeteiligung** schafft breite Legitimität und Abschreckung
✔ **Kosteneffizienz** durch Nutzung bestehender Infrastruktur
✔ **Resistenz gegen KI-Angriffe** durch nicht-internetbasierte Schlüsselübertragung
✔ **Skalierbarkeit** für globale Anwendung

Schwächen:
✗ **Kein etablierter Rahmen** – noch keine internationale Anerkennung
✗ **Koordinationskomplexität** bei dezentralen Entscheidungen
✗ **Verantwortungsdiffusion** – wer haftet bei Fehlern?
✗ **Politische Akzeptanz** noch nicht gegeben
✗ **Technische Hürden** bei Implementierung

Quellenverzeichnis

Internationale Organisationen und Abkommen

Quelle	Glaubwürdigkeit	Letzte Aktualisierung
UN General Assembly Resolution on LAWS (Dec 2, 2024)	5/5	2024
UN Secretary-General: New Agenda for Peace	5/5	2023
ASIL: Lethal Autonomous Weapons Systems & International Law	5/5	2025

Quelle	Glaubwürdigkeit	Letzte Aktualisierung
Human Rights Watch: UN Start Talks on Treaty to Ban Killer Robots	5/5	2025
Convention on Certain Conventional Weapons (CCW)	5/5	2023
International Committee of the Red Cross (ICRC)	5/5	2025

Zivilgesellschaft und NGOs

Quelle	Glaubwürdigkeit	Letzte Aktualisierung
Campaign to Stop Killer Robots	4/5	2025
156 states support UNGA resolution on autonomous weapons	4/5	2024
International Committee for Robot Arms Control (ICRAC)	4/5	2025

Europäische Union

Quelle	Glaubwürdigkeit	Letzte Aktualisierung
EU Parliament: Defence and artificial intelligence	5/5	2025
EU AI Act (Regulation 2024/1689)	5/5	2024
European Defence Fund Regulation	5/5	2021
EST: Towards Comprehensive Regulation – EU's Stance on Autonomous Weapons	4/5	2025

NATO und nationale Ansätze

Quelle	Glaubwürdigkeit	Letzte Aktualisierung
NATO: Autonomous Weapons Systems and Meaningful Human Control	4/5	2020
US DoD Directive 3000.09: Autonomy in Weapon Systems	5/5	2012 (aktualisiert)
Arms Control Association: Geopolitics and Regulation of AWS	4/5	2025

Exportkontrollen

Quelle	Glaubwürdigkeit	Letzte Aktualisierung
Wassenaar Arrangement	5/5	2025
Stimson Center: UAV Export Controls Report	4/5	2024
US Federal Register: Streamlining Export Controls for Drone Exports	5/5	2026

Trusted Web 4.0

Quelle	Glaubwürdigkeit	Letzte Aktualisierung
Nutzerkontext: Trusted Web 4.0 Konzeptbeschreibung	3/5	2026

--

Offene Fragen und Kontroversen

1. Definitionsproblematik

- **Keine einheitliche Definition** von LAWS auf internationaler Ebene
- **Grauzonen:** Was zählt als „autonom“? Was als „meaningful human control“?
- **Beispiel:** Ist ein System mit 30-sekündiger menschlicher Bestätigungsfrist noch „autonom“?

2. Umsetzungslücken

- **Dual-Use-Dilemma:** Viele Technologien haben zivile und militärische Anwendungen
- **Exportkontrollen:** Lockerungen (z.B. USA 2026) könnten Proliferation beschleunigen
- **Compliance:** Wie kann Einhaltung von Verboten überprüft werden?

3. Ethische Dilemmata

- **Abschreckung vs. Ethik:** Führt ein Verbot zu strategischen Nachteilen?
- **Asymmetrische Kriege:** Wie mit nicht-staatlichen Akteuren umgehen?
- **Autonome Verteidigung:** Sind autonome Abwehrsysteme (z.B. gegen Drohnenschwärme) ethisch vertretbar?

4. Technologische Grenzen

- **KI-Entscheidungsfähigkeit:** Können Algorithmen jemals **ethische Abwägungen** treffen?
- **Schwarmintelligenz:** Wie kann menschliche Kontrolle bei 100+ Drohnen gewahrt werden?
- **Tarnung:** Wie mit unsichtbaren Drohnen umgehen?

5. Trusted Web 4.0-spezifisch

- **Skalierbarkeit:** Funktioniert das Modell bei Millionen von Teilnehmer:innen?
- **Koordination:** Wie werden Konflikte zwischen dezentralen Akteur:innen gelöst?
- **Rechtliche Rahmenbedingungen:** Wie passt das Modell in bestehende völkerrechtliche Strukturen?
- **Finanzierung:** Wer trägt die Kosten der dezentralen Infrastruktur?

Empfehlungen und nächste Schritte

Kurzfristig (2026-2027)

Für Staaten und internationale Organisationen:

1. **UN-GGE LAWS beschleunigen: Verbindliches Abkommen bis 2026** für LAWS ohne menschliche Kontrolle
2. **Definitionen klären:** Einigung auf **international akzeptierte Definitionen** von LAWS und MHC
3. **Exportkontrollen stärken: Schließung von Lücken** im Wassenaar-Arrangement und MTCR
4. **Finanzierungsverbote ausweiten:** EU-Ansatz auf **globale Ebene** übertragen

Für die EU:

1. **Militärische KI in AI Act integrieren: Lücke schließen** durch Erweiterung des Anwendungsbereichs
2. **EDF-Kriterien verschärfen: Strengere Anforderungen** an menschliche Kontrolle
3. **Bürgerbeteiligung fördern: Pilotprojekte** für digitale Wehrpflicht nach Trusted Web 4.0-Modell

Für NATO:

1. **Einheitliche Standards: Verbindliche MHC-Richtlinien** für alle Mitgliedstaaten
2. **Abwehr gegen Drohnenschwärme:** Entwicklung **autonomer Abwehrsysteme** mit menschlicher Aufsicht

Mittelfristig (2027-2030)

Für internationale Gemeinschaft:

1. **Verifikationsmechanismen:** Entwicklung von **Technologien zur Überprüfung** von LAWS-Einsätzen
2. **Accountability-Frameworks:** Klärung der **Haftungsfragen** bei autonomen Systemen
3. **Zivilgesellschaft einbinden:** **Regelmäßige Konsultationen** mit NGOs und Expert:innen

Für Trusted Web 4.0:

1. **Pilotimplementierung:** **Testphase** in einem EU-Mitgliedstaat (z.B. Estland, Finnland)
2. **Technische Machbarkeit:** Entwicklung der **WAN-anonymen Kommunikationsinfrastruktur**
3. **Rechtlicher Rahmen:** **Anpassung an völkerrechtliche Anforderungen**
4. **Internationale Kooperation:** **Partnerschaften** mit gleichgesinnten Staaten

Langfristig (ab 2030)

1. **Globales Regime:** **Umfassendes Abkommen** ähnlich dem Chemiewaffenübereinkommen
2. **KI-Governance:** **Internationale KI-Agentur** für militärische Anwendungen
3. **Dezentrale Verteidigung:** **Integration** von Trusted Web 4.0-Konzepten in nationale Verteidigungsstrategien
4. **Bildung und Sensibilisierung:** **Globale Kampagnen** zur Aufklärung über Risiken autonomer Waffen

Fazit

Die **internationale Gemeinschaft** hat in den letzten Jahren **erhebliche Fortschritte** bei der Anerkennung der ethischen und rechtlichen Herausforderungen autonomer Waffensysteme gemacht. Die **UN-Resolution von 2024** und die **EU-Finanzierungsverbote** zeigen, dass ein **globaler Konsens** über die Notwendigkeit menschlicher Kontrolle besteht. Allerdings bleiben **Definitionslücken, Umsetzungsprobleme und geopolitische Spannungen** bestehen.

Trusted Web 4.0 bietet einen **radikal neuen Ansatz**, der die **Schwächen zentraler Regulierung** durch **Dezentralisierung und Bürgerbeteiligung** überwinden könnte. Das Modell ist **theoretisch überzeugend** und könnte **kosteneffizienter und resilienter** sein als traditionelle Ansätze. Allerdings fehlt es noch an **praktischer Umsetzung und internationaler Anerkennung**.

Die größte Herausforderung bleibt die **Vereinbarkeit von Sicherheit und Ethik** in einer Welt, in der autokratische Staaten autonomer Waffen als Mittel der **Machtprojektion und Unterdrückung** nutzen. Die nächsten Jahre werden zeigen, ob die internationale Gemeinschaft in der Lage ist, **wirksame Mechanismen** zu entwickeln, die sowohl **militärische Notwendigkeiten** als auch **menschliche Werte** berücksichtigen.

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!

