

SWP-WebMonitor

Cybersicherheit und Digitalpolitik

Nr. 2/2026

SWP-Informationsservices

Mark Schrolle, 24.03.2026

Der SWP-WebMonitor Cybersicherheit und Digitalpolitik ist ein unentgeltliches, kompaktes Informationsprodukt mit ausgewählten Hinweisen auf aktuelle Dokumente und Analysen zu cyber- und digitalpolitisch relevanten Fragen und Entwicklungen. Alle Titel sind mit einem Link versehen, der meist direkt zum Volltext führt. Die aufgelisteten Beiträge sind nach Erscheinungsdatum sowie nach Namen der herausgebenden Institution in alphabetischer Reihenfolge sortiert. Grundlage der Erstellung ist ein überwiegend festgelegtes Set an Quellen, zumeist von Thinktanks und Forschungsinstituten. Die Auswahl orientiert sich am Bedarf des [Forschungsclusters Cybersicherheit und Digitalpolitik](#) der SWP. Der Auswahl-Fokus liegt auf wissenschaftlichen bzw. wissenschaftlich basierten Beiträgen. Der WebMonitor wird i.d.R. einmal im Monat erstellt, nicht aber bei Abwesenheit des Bearbeiters.

Inhaltsverzeichnis

SWP-Publikationen

Globale Technologiepolitik

Internet Governance

Untersee-Datenkabel

Satelliten Internet

Menschenrechte im digitalen Raum

US-Technologiepolitik

EU-Digitalpolitik

Cybersicherheit

Cybersicherheitspolitik

Cyberdiplomatie

Cyberkriminalität

Cyber intrusion capabilities

Cybersicherheit von neuen Technologien

EU-Cybersicherheit

Technologie & Streitkräfte

Cybersicherheit im Militär

Militärische Cyberfähigkeiten

Neue Technologien im Militär

Neue Technologien

Künstliche Intelligenz (KI)

Biotechnologie

EU-Governance

Digitale Währungen

SWP-Publikationen

[Cyber Activity Balance 2025: The EU in Focus - Situational Awareness based on European Repository on Cyber Incidents \(EuRepoC\)](#)

Annegret Bendiek, Jonas Hemmelskamp, Lena Rottinger
Stiftung Wissenschaft und Politik (SWP), 02.2026, 14 Seiten.

[Technologie- und Cybersicherheitspolitik ohne, gegen, mit Washington. Europas Handlungsmöglichkeiten im Konfliktfall](#)

Alexandra Paulus, Daniel Voelsen
In: Mit, ohne, gegen Washington: Die Neubestimmung der Beziehungen Europas zu den USA, S. 23–27
Stiftung Wissenschaft und Politik (SWP), 22.01.2026

[Zurück zum Inhaltsverzeichnis](#)

Globale Technologiepolitik

Internet Governance

[‘It’s a myth that Chinese internet users are mindless automatons’](#)

Yi-Ling Liu, Isabella Wilkinson
Chatham House, 16.03.2026

[Chinese De-Risking: Europe Needs to Accelerate](#)

Valentin Weber
Center for European Policy Analysis, 05.03.2026

[South Korea’s Online Platform Fairness Bill](#) - A New Digital Nontariff Barrier in U.S.-ROK Trade

Nigel Cory
National Bureau of Asian Research, 25.02.2026, 8 Seiten.

[Cross-Border Data Transfer Regimes: Current Landscape and Outlook Ahead](#)

S. Yash Kalash
Centre for International Governance Innovation (CIGI), 24.02.2026, 36 Seiten.

[Conference Highlights: UN Open Source Week 2025 - An Open Community for the Global Digital Compact](#)

Sachiko Muto
OpenForum Europe, 05.02.2026, 48 Seiten.

[Zurück zum Inhaltsverzeichnis](#)

Untersee-Datenkabel

[Risk Beneath the Waves: Safeguarding Subsea Cables for a Secure Global Network](#)

Romina Bandura, Erin Murphy, Thomas Bryja

Center for Strategic and International Studies (CSIS), 05.03.2026

[Zurück zum Inhaltsverzeichnis](#)

Satelliten Internet

[The Satellite Encryption Gap: Why Everyday Citizens' Communications Are at Risk](#)

Lauryn Williams, Kuhu Badgi

Center for Strategic and International Studies (CSIS), 06.03.2026

[How Russia Is Intercepting Communications from European Satellites](#)

Aleix Nadal Campos

RAND Corporation, 02.03.2026

[Building a European competitive edge in space](#) - An agenda for action

Carlo Des Dorides, Andrea G. Rodríguez, Jaime Martínez, Christopher Schade

Centre for European Policy Studies (CEPS), 05.03.2026, 25 Seiten.

[Room for Change? Premises of the EU's Space Policy](#)

Dorthea Gradek

Norwegian Institute for International Affairs (NUPI), 24.02.2026

[A Quick Note on Orbiting Data Centers](#)

James Lewis

Center for European Policy Analysis, 05.02.2026

[Maintaining the Space Edge: Strategic Reforms for U.S. Dominance in Low Earth Orbit](#)

Taylor Rajic, Lauryn Williams, Matt Pearl

Center for Strategic and International Studies (CSIS), 02.02.2026

[Zurück zum Inhaltsverzeichnis](#)

Menschenrechte im digitalen Raum

[The Architecture of Digital Repression](#)

Irene Poetranto

Carnegie Endowment for International Peace, 10.03.2026

[China's AI-Empowered Censorship: Strengths and Limitations](#)

Nathan Law

Carnegie Endowment for International Peace, 10.03.2026

[Von personalisierter Werbung zur staatlichen Verfolgung - Zweckbindung als Grundrechtsschutz im Zeitalter von KI](#)

Rainer Mühlhoff, Hannah Ruschemeier

Verfassungsblog | On Matters Constitutional, 03.02.2026

[Zurück zum Inhaltsverzeichnis](#)

US-Technologiepolitik

[Private Power, Public Values](#) - Anthropic and the Constitutional Dimension of Governance in the Digital Environment

Lucas Henrique Muniz de Conceição

Verfassungsblog | On Matters Constitutional, 11.03.2026

[The Emerging US Influence Threat to British Democracy](#)

Neil Barnett, Eliza Lockhart

Royal United Services Institute (RUSI), 26.02.2026

[The Pentagon/Anthropic Clash Over Military AI Guardrails](#)

Jessica Dorsey, et al.

Opinio Juris, 26.02.26

[America's Digital Empire Has a Trust Problem](#)

Kat Duffy

Council on Foreign Relations, 24.02.2026

[Der neue Davos Man](#)

Cord Jakobeit

Journal für Internationale Politik und Gesellschaft | IPG Journal, 03.02.2026, 5 Seiten.

[Tech Dependencies Undermine UK National Security](#)

Sophie Williams-Dunning

Royal United Services Institute (RUSI), 02.02.2026

Tech Diplomacy for a New Global Order

Alexander Kleibrink

German Marshall Fund of the United States, 23.01.2026

[Zurück zum Inhaltsverzeichnis](#)

EU-Digitalpolitik

EU-UK digital cooperation

Maria Niestadt

European Parliamentary Research Service, 15.03.2026

The New Containment Doctrine: How the United States Is Using Trade to Stop Digital Regulation

Philip Luck, Duc Minh Nguyet (Moon) Nguyen

Center for Strategic and International Studies (CSIS), 09.03.2026

From pledges to practice: The Digital Services Act at two years

Anh Nguyen

Hertie School Centre for Digital Governance, 05.03.2026

The case for a European Union digital enforcement authority

Mario Mariniello

Bruegel, 05.03.2026, 16 Seiten.

Europe's Expanding Digital Partnerships

Anda Bologna

Center for European Policy Analysis, 04.03.2026

A Transatlantic Tech Partnership

Dylan Welch, Sharinee Jagtiani

German Marshall Fund of the United States, 27.02.2026

Cuando entrar es fácil, pero salir imposible: la asimetría regulatoria que frena la inversión digital en Europa

Judith Arnal

Real Instituto Elcano, 25.02.2026, 60 Seiten.

One Tech Policy Battle After Another

Ronan Murphy

Center for European Policy Analysis, 12.02.2026

Leaders' retreat: EU needs escape velocity to close tech gap with US, China

Paweł Świeboda

European Policy Centre, 05.02.2026

Power in Numbers: Governments Gang Up On Tech

Clara Riedenstein

Center for European Policy Analysis, 04.02.2026

OSOR Handbook: Open Source Software in Public Administration

Axel Thévenet, Ciarán O'Riordan, Jaakko Karhu, Sivan Pätsch

OpenForum Europe, 04.02.2026, 45 Seiten.

Progress and trends in the national open source policies and legal frameworks

Éléonore Daxhelet, Jaakko Karhu

OpenForum Europe, 04.02.2026, 27 Seiten.

EU-Africa Digital Partnership

Niels Keijzer, et al.

Istituto Affari Internazionali, 02.02.2026

Europe's Bazooka Could Hit US Tech

William Echikson, Ronan Murphy

Center for European Policy Analysis, 23.01.2026

To Regulate or Not to Regulate? - The EU, ICT, and the Merits of a Geopolitical Approach

Paolo Passaglia

Völkerrechtsblog, 19.01.2026

[*Zurück zum Inhaltsverzeichnis*](#)

Cybersicherheit

Cybersicherheitspolitik

South Korea's Integrated Cyber Defense Framework: Active Cyber Defense and Reactive Responses

Sunha Bae

Center for Strategic and International Studies (CSIS), 20.03.2026, 23 Seiten.

Wartime Ukraine offers global lessons on the future of cyber resilience

Oleksandr Bakalynskyy, Maggie McDonough
Atlantic Council, 19.03.2026

Germany's new Cyber Active Defense Law - Written Statement on the "Gesetz zur Stärkung der Cybersicherheit"

Sven Herpig
Interface, 18.03.2026, 9 Seiten.

America's AI Cyber Defense Gap Needs Congress to Act

Spencer Michaels, Janet Egan, Michael Daniel
Center for a New American Security, 17.03.2026

Trump's Cyber Strategy Falls Short on China, Iran, and the Threats That Matter Most

Matthew Ferren
Council on Foreign Relations, 16.03.2026

Brief, Bold and Beautiful? Reactions on the US National Cyber Strategy

Louise Marie Hurel, et al.
Royal United Services Institute (RUSI), 16.03.2026

What Does the New Cyber Strategy Really Mean?

Emily Harding
Center for Strategic and International Studies (CSIS), 09.03.2026

Infinite Potential—Insights from the Cyber Surprise Scenario - Post-Series Scenario

Report from a Sequence of Day After Artificial General Intelligence Exercises
George Hage, et al.
RAND Corporation, 09.03.2026

North Korean and Russian cyber actors may be teaming up. So must allies

Joseph Jarnecki, Pia Hüscher
Royal United Services Institute (RUSI), 06.03.2026

Securing Cyberspace in the Middle East: An Actionable Blueprint

Bassant Hassib
Observer Research Foundation (ORF), 05.03.2026

Strengthening UK-South Korea Cyber Security Cooperation

Pia Hüscher, Joseph Jarnecki
Royal United Services Institute (RUSI), 02.03.2026

[The Middle-Ground Amidst Great \(Cyber\) Power Competition: From Pawns to King-makers?](#)

Arthur Laudrain

Center for Security Studies (CSS) | ETH Zürich, 21.02.2026

[Towards a British Approach to Cyber Campaigning](#)

Richard J. Harknett, Monica Kello

Royal United Services Institute (RUSI), 10.02.2026

[Cyber Conflicts and the Erosion of Institutional Trust: the Impacts on Citizens](#)

Claudia Schettini

Istituto per gli studi di politica internazionale (ISPI), 05.02.2026

[A Silent Arsenal: State Hacking and the Emerging Digital Order](#)

Ludovica Favarotto, Claudia Schettini

Istituto per gli studi di politica internazionale (ISPI), 05.02.2026

[“State Hacking”: What Is it and Who Is Behind it?](#)

Luigi Martino

Istituto per gli studi di politica internazionale (ISPI), 05.02.2026

[State Hacking in the Age of Artificial Intelligence](#)

Nori Katagiri

Istituto per gli studi di politica internazionale (ISPI), 05.02.2026

[Japan Goes on the Offensive in Cybersecurity](#)

Rintaro Nishimura

Istituto per gli studi di politica internazionale (ISPI), 05.02.2026

[Rebooting the UK's Cyber Strategy](#)

Joseph Jarnecki Jamie MacColl

Royal United Services Institute (RUSI), 03.02.2026

[Cybersecurity in 2026: How AI will reshape the Digital Battlefield](#)

Soumya Awasthi

Observer Research Foundation (ORF), 31.01.2026

[The US needs a cybersecurity roadmap](#)

Franklin D. Kramer, Robert J. Butler, Melanie J. Teplinsky

Atlantic Council, 29.01.2026

[Zurück zum Inhaltsverzeichnis](#)

Cyberdiplomatie

[Resetting Cyber Relations with the United States](#)

Patryk Pawlak, Chris Painter

Carnegie Endowment for International Peace, 10.03.2026

[The UN's New Global Mechanism on Cybersecurity](#)

Christina Rupp

Interface, 06.03.2026

[Assessing the impact of counter-ransomware interventions](#)

Jamie MacColl, Sophie Williams-Dunning, Max Smeets

Royal United Services Institute (RUSI), 05.03.2026

[Shaping the UN Cybercrime Convention: Human Rights at a Crossroads](#)

Samaya Anjum, Jason Pielemeier, Elonnai Hickok

EU Cyber Direct, 12.02.2026

[Russia's multilateral cyber norm promotion: The duality of great power projection and digital authoritarianism](#)

Sinikukka Saari, Flavia Lucenti

Finnish Institute of International Affairs (FIIA), 25.12.2025

[Zurück zum Inhaltsverzeichnis](#)

Cyberkriminalität

[Cyber-hacks are eroding our economy – tech firms and boardrooms must bolster their defences](#)

Joseph Jarnecki, Jamie MacColl

Royal United Services Institute (RUSI), 20.02.2026

[Responding to AI-Enabled Cybercrime: Governance, Attribution, and Escalation](#)

Helena Yixin Huang

S. Rajaratnam School of International Studies, 26.01.2026, 4 Seiten.

[Zurück zum Inhaltsverzeichnis](#)

Cyber intrusion capabilities

[Mythical Beasts: Investigating the role of intermediaries in the proliferation of offensive cyber capabilities](#)

Jen Roberts, Sarah Graham, Lyla Renwick-Archibold
Atlantic Council, 18.03.2026, 13 Seiten.

[The role of cyber-proxy in cyber threat intelligence](#)

Francesco Schifilliti
Istituto per gli studi di politica internazionale (ISPI), 05.02.2026

[Zurück zum Inhaltsverzeichnis](#)

Cybersicherheit von neuen Technologien

[Fighting AI Cyberattacks Starts with Knowing They're Happening](#)

Janet Egan, Michelle Nie
Center for a New American Security, 26.02.2026

[Agentic Artificial Intelligence and Cyberattacks](#)

Kelley M. Sayler, Catherine A. Theohary
Congressional Research Service Reports, 03.02.2026

[Zurück zum Inhaltsverzeichnis](#)

EU-Cybersicherheit

[Cold War: Moscow Targets Europe's Communal Heating](#)

Miro Sedlák
Center for European Policy Analysis, 16.03.2026

[Enter Europe's Cyber Deterrence](#)

Alexander Klimburg
Center for Strategic and International Studies (CSIS), 10.03.2026, 22 Seiten.

[A Joint Cyber Defense for Europe?](#)

Marija Golubeva
Center for European Policy Analysis, 03.03.2026

When Red Lines Cross Blue Lines: Cyber Attacks on Poland's Water Infrastructure – Part I

Szymon Skalski, Natosha Hoduski
Lieber Institute West Point, 02.03.2026

ENISA International Strategy 2026

European Union Agency for Cybersecurity (ENISA), 09.02.2026, 8 Seiten.

Europe's New Cyber Rules Target China — and US

Ieva Ilves
Center for European Policy Analysis, 22.01.2026

[Zurück zum Inhaltsverzeichnis](#)

Technologie & Streitkräfte

Cybersicherheit im Militär

Active Cyber Defense in the Korean Context

James Andrew Lewis
Center for Strategic and International Studies (CSIS), 12.03.2026, 11 Seiten.

Alliance Under Fire: Ukraine's Swift Public-Private Response to Protect Vital Infrastructure

Stefan Soesanto
Istituto per gli studi di politica internazionale (ISPI), 05.02.2026

Cybersecurity of weapon systems: international law requirements and technical standards

Aleksi Kajander, Rain Liivoja, Maarja Naagel
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2025

[Zurück zum Inhaltsverzeichnis](#)

Militärische Cyberfähigkeiten

Demystifying Iranian Cyber Operations in the U.S.-Iran Conflict

Nikita Shah
Center for Strategic and International Studies (CSIS), 20.03.2026

Cyber Warfare and the Limits of International Criminal Law: Can Digital Attacks Amount to War Crimes?

Mahmoud Abdelwahab
Opinio Juris, 19.03.2026

Shamoon Strikes Stryker: Iran Wields Wiper Attacks

Emily Otto
Center for European Policy Analysis, 16.03.2026

Interview: Large countries have a silent deterrent – Finland, too, has an offensive capability that is not talked about

Pia Hüscher
Royal United Services Institute (RUSI), 14.03.2026

Fog, Proxies and Uncertainty: Cyber in US-Israeli Operations in Iran

Louise Marie Hurel
Royal United Services Institute (RUSI), 05.03.2026

How Will Cyber Warfare Shape the U.S.-Israel Conflict with Iran?

Lauryn Williams, Kuhu Badgi
Center for Strategic and International Studies (CSIS), 03.03.2026

Control, Alt, Influence: the Potential for US Cyber Operations in Iran

Prerana Joshi
Royal United Services Institute (RUSI), 19.02.2026

The Cyber Arsenal: North Korea's Silent Power

Ludovica Favarotto
Istituto per gli studi di politica internazionale (ISPI), 05.02.2026

Forward Defense in Cyberspace: Iran's Hybrid State-Hacking Doctrine

Luigi Toninelli
Istituto per gli studi di politica internazionale (ISPI), 05.02.2026

A Coming-Out Party for US Cyber Deterrence?

Allison Pytlak
Stimson Center, 28.01.2026

Enabling NATO Digital Capabilities - Lessons from Swedish investment in digital capabilities for defence

Erik Silfversten, et al.
RAND Corporation, 21.01.2026

[Enabling NATO Digital Capabilities](#) - Lessons from Finnish investment in digital capabilities for defence
Erik Silfversten, et al.
RAND Corporation, 21.01.2026

[Poland's Digital Defence Landscape](#) - Lessons from Polish investment in digital capabilities for defence
Erik Silfversten, et al.
RAND Corporation, 21.01.2026

[Small State, Digital Giant](#) - Lessons from Estonian investment in digital capabilities for defence
Erik Silfversten, et al.
RAND Corporation, 21.01.2026

[Zurück zum Inhaltsverzeichnis](#)

Neue Technologien im Militär

[Legal Accountability for AI-Driven Autonomous Weapons](#)
Gerald Mako
Lieber Institute West Point, 09.03.2026

[Setting the Rules for AI Warfare](#)
Paul Scharre
Center for a New American Security, 04.03.2026

[\(Ir-\)Responsible by Design? Corporate Guardrails and the Governance of Military AI](#)
Jessica Dorsey, et al.
Opinio Juris, 02.03.26

[Taiwan in the Hidden War: The Contest for Technological Sovereignty Against Infiltration](#)
Federica Bagna, Yi-Chieh Chen, Niklas Swanström
Institute for Security and Development Policy, 03.2026, 60 Seiten.

[AI in Modern Warfare: India's Strategic Challenges and Opportunities](#)
Manoj Joshi
Observer Research Foundation (ORF), 27.02.2026

[Military AI Adoption Is Outpacing Global Cooperation](#)
Michael C. Horowitz
Council on Foreign Relations, 11.02.2026

[How Russia Is Reshaping Command and Control for AI-Enabled Warfare](#)

Kateryna Bondar

Center for Strategic and International Studies (CSIS), 10.02.2026, 22 Seiten.

[Tech Cooperation and Tech Sovereignty in the New World Order](#)

Valentin Weber, Katja Muñoz

Deutsche Gesellschaft für Auswärtige Politik (DGAP), 09.02.2026, 4 Seiten.

[The New Frontline: Technology Is a Modern Warfighting Domain](#)

Katrina Schweiker

Center for Strategic and International Studies (CSIS), 02.02.2026

[China's Military AI Wish List](#) - This report examines thousands of Chinese-language open-source requests for proposal (RFPs) published by the People's Liberation Army between January 1, 2023, and December 31, 2024.

Emelia Probasco, Sam Bresnick, Cole McFaul

Center for Security and Emerging Technology (CSET), 02.2026, 42 Seiten.

[China and the Ethics of Military AI: Debating the Norms of Future Wars](#)

Ilaria Carrozza, Bjørnar Sverdrup-Thygeson

Peace Research Institute Oslo (PRIO), 30.01.2026, 16 Seiten.

[Emerging Technologies and the Enduring Elements of Warfare](#)

Ivan Zaccagnini

Center for Security Studies (CSS) | ETH Zürich, 12.03.2026, 24 Seiten.

[Report on the Conference on the Law Applicable to the Use of Biometrics by Armed Forces in Tallinn, 23-24 October](#)

Aleksi Kajander, Marten Zwanenburg, Natalia Myshina

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 02.2026, 21 Seiten.

[AI in Chinese, Indian and US Nuclear Postures, Norms and Systems](#)

Lora Saalman

Stockholm International Peace Research Institute (SIPRI), 02.2026, 38 Seiten.

[Responsible Procurement of Military Artificial Intelligence](#)

Vincent Boulanin, Netta Goussac

Stockholm International Peace Research Institute (SIPRI), 02.2026, 39 Seiten.

[Addressing Multidomain Nuclear Escalation Risk](#)

Wilfred Wan

Stockholm International Peace Research Institute (SIPRI), 01.2026, 12 Seiten.

[Zurück zum Inhaltsverzeichnis](#)

Neue Technologien

Künstliche Intelligenz (KI)

[Box-ticking will never ensure AI safety](#)

Abeera Dubey
Hertie School Centre for Digital Governance, 15.03.2026

[Sovereignty, safety, and scale: Takeaways from the India AI Impact Summit](#)

Cameron F. Kerry, Elham Tabassi
Brookings Institution, 12.03.2026

[AI and Robotics: National Security Implications](#)

Megan Hughes
Centre for Emerging Technology and Security (CETaS), 12.03.2026, 21 Seiten.

[Reality Checking a Major National R&D Investment in AI Trustworthiness, Safety, and Security](#) - Weighing the Costs and Benefits of a \$10 Billion Bet on Increasing the Robustness of the United States' AI Future

Brian A. Jackson, Pauline Moore
RAND Corporation, 12.03.2026

[AI Cooperation Trajectories: Adversaries and Geostrategic Competitors](#)

Tony A., Megan Hughes
Centre for Emerging Technology and Security (CETaS), 09.03.2026, 45 Seiten.

[The Indo-Pacific as the Epicenter of AI Risk](#)

Husan Chahal
National Bureau of Asian Research, 09.03.2026

[KI und hybride -Bedrohungen 2.0](#) - Warum Deutschland jetzt -handeln muss

Katja Muñoz
Deutsche Gesellschaft für Auswärtige Politik (DGAP), 04.03.2026, 13 Seiten.

[From Delhi to Geneva, what's next for AI governance?](#)

Konstantinos Komaitis
Digital Forensic Research Lab (DFR Lab), 04.03.2026

[Can the Transatlantic Community Align on AI Safety?](#)

Adrienne Goldstein
German Marshall Fund of the United States, 03.03.2026

[AI Summitry — Growth Beats Safety](#)

Anda Bologna
Center for European Policy Analysis, 03.03.2026

[Is AI sovereignty possible? Balancing autonomy and interdependence](#)

Brooke Tanner, et al.
Brookings Institution, 17.02.2026, 72 Seiten.

[The Weapons of Mass Destruction AI Security Gap](#)

Cassidy Nelson
RAND Corporation, 12.02.2026

[AI Security Guide and Risk Assessment Tool](#)

Karen Schwindt, et al.
RAND Corporation, 12.02.2026

[International AI Safety Report 2026](#)

Carnegie Endowment for International Peace, 03.02.2026

[Tipping the Cyber Balance: How AI Benchmarks Could Make Software Safer](#)

Gopal P. Sarma, Kathleen Fisher
RAND Corporation, 03.02.2026

[AI risks from non-state actors](#)

Kyle Chan, Michael E. O'Hanlon, Qi Haotian, Zheng Lefeng
Brookings Institution, 29.01.2026

[Four Governance Approaches to Securing Advanced AI](#)

Ian Mitch, et al.
RAND Corporation, 23.01.2026

[The HAIP Reporting Framework: Its value in global AI governance and recommendations for the future](#)

Miranda Bogen, et al.
Brookings Institution, 21.01.2026, 4 Seiten.

[Zurück zum Inhaltsverzeichnis](#)

Biotechnologie

[Two Illegal Biolabs Reveal Gaps in U.S. Biosecurity](#)

Sam Howell
Center for a New American Security, 18.03.2026

[Tech-Prioritäten in Chinas Fünfjahresplan](#) - Europa muss sich auf den Wettbewerb in

Biomanufacturing vorbereiten

Michael Laha
Deutsche Gesellschaft für Auswärtige Politik (DGAP), 11.03.2026, 5 Seiten.

AI-Ready Biodata Is America's Next Strategic Infrastructure

Michelle Holko, Sam Howell
Center for a New American Security, 09.03.2026

IP26033 | Voluntary Weapons Control: Private Companies and Global Bio-governance

Dirk van der Kley
S. Rajaratnam School of International Studies, 03.03.2026, 6 Seiten.

Preventing Biological Weapons Proliferation: Operational Applications of Emerging Technologies

Miranda Smith, Kolja Brockmann, Mark Bromley
Stockholm International Peace Research Institute (SIPRI), 03.2026, 36 Seiten.

Europe Is Betting on Biotech—But Success Depends on Demand

Sarah Parkinson, Sana Zakaria, Nick Fahy
RAND Corporation, 27.02.2026

Governing Biotechnology's Dual-Use Security Dilemma

Lakshmy Ramakrishnan
Observer Research Foundation (ORF), 20.02.2026

Neurotechnology deserves an EU research moonshot

Paweł Świeboda
Centre for Future Generations, 19.02.2026

America's Key to Biotechnology Leadership? AI-Ready Biodata.

Sam Howell, Michelle Holko
Center for a New American Security, 13.02.2026

Developing a Risk-Scoring Tool for Artificial Intelligence-Enabled Biological Design

- A Method to Assess the Risks of Using Artificial Intelligence to Modify Select Viral Capabilities
Roger Brent, et al.
RAND Corporation, 11.02.2026

Measuring Biological Capabilities and Risks of AI Agents - Generating and Interpreting

Evidence from Agentic Evaluations
Kyle Brady, Alyssa Worland, Jeffrey Lee, Patricia Paskov
RAND Corporation, 10.02.2026

Prioritizing Feasible and Impactful Actions to Enable Secure AI Development and Use in Biology

Josh Dettman, et al.
RAND Corporation, 21.01.2026

[Zurück zum Inhaltsverzeichnis](#)

EU-Governance

AI Diplomacy for a Multipolar World - Europe's Moment to Act on Trusted AI Partnerships

Maaïke Heijmans, Alexandre Ferreira Gomes
Clingendael, 18.03.2026, 10 Seiten.

Building a centralised national AI authority

Jan Króliński
Interface, 12.03.2026

A Br(AI)ghter Future for the EU? Shaping EU Strategy in the Era of General Artificial Intelligence

Aleksandra Wójtowicz
Polish Institute of International Affairs (PISM), 26.02.2026, 13 Seiten.

From Common Worries to Digital Commons - How Europe Can Stop Renting Clouds and Build Its Own

Alexandre Ferreira Gomes, Maaïke Heijmans, Jelle van den Wijngaard
Clingendael, 24.02.2026, 31 Seiten.

Die KI-Schulungspflicht sollte praxisnah reformiert werden - Artikel 4 der KI-Verordnung: Gut für die Bürokratie, schlecht in der Praxis

Leonie Mader
Konrad Adenauer Stiftung, 20.02.2026, 2 Seiten.

Digital Omnibus on AI [EU Legislation in Progress]

Maria Niestadt
European Parliamentary Research Service, 12.02.2026

European AI FOMO - The European Commission Sacrifices the Digital Acquis at the Altar of AI Hype

Felix Bieker, Katherine Nolan
Verfassungsblog | On Matters Constitutional, 29.01.2026

Lost in Definition: How Confusion over Agentic AI Risks Governance

Yasir Atalan, Ian Reynolds, Benjamin Jensen
Center for Strategic and International Studies (CSIS), 26.01.2026, 7 Seiten.

[Zurück zum Inhaltsverzeichnis](#)

Digitale Währungen

[Stablecoin rails and the limits of financial power](#)

Julia Voo

International Institute for Strategic Studies (IISS), 05.03.2026

[Payment sovereignty without walls: the case for Europe's multi-rail ecosystem](#)

Judith Arnal

Centre for European Policy Studies (CEPS), 27.02.2026, 17 Seiten.

[Global Payment Infrastructure: Moving from Multi-Rail to Full-Stack Systems](#)

S. Yash Kalash

Centre for International Governance Innovation (CIGI), 26.02.2026

[Dinero digital y poder: tensiones del nuevo orden monetario global](#)

Federico Steinberg, Carlos Sánchez Reboiro

Real Instituto Elcano, 18.02.2026

[Zurück zum Inhaltsverzeichnis](#)

--

Mark Schrolle

M.A.

Referat Informationsservices | Information Services

Informations- und Datenmanager | Information and Data Manager

Tel. +49 30 88007-553

mark.schrolle@swp-berlin.org

Stiftung Wissenschaft und Politik

German Institute for International and Security Affairs

Ludwigkirchplatz 3-4, 10719 Berlin

<https://www.swp-berlin.org/>

bsky.app/profile/swp-berlin.org

[linkedin.com/company/swp-berlin](https://www.linkedin.com/company/swp-berlin)