eoss-conf.com

ISSUE
№76

EUROPEAN OPEN SCIENCE SPACE

COLLECTION OF SCIENTIFIC PAPERS

4TH INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

SCIENTIFIC RESEARCH: MODERN INNOVATIONS AND FUTURE PERSPECTIVES

FEBRUARY 23-25, 2026
MONTREAL, CANADA

EUROPEAN OPEN SCIENCE SPACE

Proceedings of the 4th International Scientific and Practical Conference

"Scientific Research: Modern Innovations and Future Perspectives"

February 23-25, 2026

Montreal, Canada

Collection of Scientific Papers

Montreal, 2026

UDC 01.1

Collection of Scientific Papers with the Proceedings of the 4th International Scientific and Practical Conference «Scientific Research: Modern Innovations and Future Perspectives» (February 23-25, 2026, Montreal, Canada). European Open Science Space.

ISBN 979-8-89704-956-1 (series)
DOI 10.70286/EOSS-23.02.2026

The conference is included in the Academic Research Index ReserchBib International catalog of scientific conferences.

The conference is registered in the database of scientific and technical events of UkrISTEI to be held on the territory of Ukraine (Certificate №1053 dated 22.12.2025).

The materials of the collection are presented in the author's edition and printed in the original language. The authors of the published materials bear full responsibility for the authenticity of the given facts, proper names, geographical names, quotations, economic and statistical data, industry terminology, and other information.

ISBN 979-8-89704-956-1

EUROPEAN OPEN SCIENCE SPACE

Humanities and Social Sciences Communications, 11(1), 101. https://doi.org/10.1057/s41599-024-02605-5
9. Humprecht, E. (2025). The role of trust and attitudes toward democracy in the dissemination of disinformation: A comparative analysis of six democracies. Digital Journalism. https://doi.org/10.1080/21670811.2023.2200196
10. Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S., & Lewandowsky, S. (2022). Psychological inoculation improves resilience against misinformation on social media. Science Advances, 8(34), eabo6254. https://doi.org/10.1126/sciadv.abo6254

DOI 10.70286/EOSS-23.02.2026.005.172-174

THE INSTITUTIONAL AND NORMATIVE DIMENSION OF GLOBAL CYBER GOVERNANCE IN THE UNITED STATES OF AMERICA

Nepochatov Danylo
PhD Student
Kuz Oleh
Doctor of Philosophy, Professor
Department of International Relations and Political Philosophy
Simon Kuznets Kharkiv National University of Economics, Ukraine

The United States of America plays the role of a fundamental architect of modern cyberspace, which provides it with an indisputable structural advantage in global digital governance. Historically acting as the "cradle" of the internet, the US laid the foundation for this global network back in 1968 with the creation of ARPANET – an experimental computer system funded by the Advanced Research Projects Agency (ARPA) of the US Department of Defense. The initial goal, which was to connect the computers of Pentagon research centers via telephone lines, evolved into the creation of a comprehensive digital environment. As of 2023, according to the International Telecommunication Union, internet penetration among US citizens reached 93.6%, confirming the deep integration of digital technologies into all spheres of social life [1].

The institutional design of US national cyber governance is complex and relies on an extensive system of specialized agencies. A key regulatory function is performed by the Federal Communications Commission (FCC), an independent agency established in 1934 that oversees interstate and international communications and has jurisdiction over the entire national territory [2]. Another important element of the governance architecture is the National Telecommunications and Information Administration (NTIA) within the Department of Commerce, whose functionality is focused on advising the government on telecommunications policy and digital economy development [1].

The evolution of the US regulatory and legal landscape vividly reflects the gradual securitization of the cyber sphere. In the early stages, the key instruments for countering threats were the Computer Fraud and Abuse Act (CFAA, 1986), which criminalized unauthorized access to systems, and the Computer Security Act (1987), which introduced security standards for federal agencies [3]. In the 1990s, the focus shifted to regulating ethical norms and protecting intellectual property, which materialized in the Communications Decency Act (CDA, 1996) and the Digital Millennium Copyright Act (DMCA, 1998) [4].

Since the early 2000s, the US strategy has reoriented towards the proactive protection of critical infrastructure amidst growing risks of technological confrontation. The National Institute of Standards and Technology (NIST) developed basic framework documents, and the Cybersecurity Information Sharing Act (CISA, 2015) institutionalized interaction between the public and private sectors [5]. A landmark stage was the creation in 2018 of the Cybersecurity and Infrastructure Security Agency (CISA), which consolidated national efforts to protect against attacks by integrating the United States Computer Emergency Readiness Team (US-CERT) [2].

In this context, the US institutional architecture plays a critical role not only in passive technical defense but also in transforming cyber diplomacy into a full-fledged narrative arena. The mechanism of diplomatic attribution—the political and legal establishment of responsibility for cyber incidents—acquires special strategic significance. Utilizing the expertise of CISA and the intelligence community, the US integrates attribution into its strategic communications to counter non-state actors: hacker syndicates, transnational media structures, and cyber proxies conducting psychological and information operations. In the conditions of cognitive confrontation in cyberspace, public attribution allows not only to delegitimize the subversive activities of such non-state entities but also to exert normative pressure on sovereign states that covertly sponsor their actions.

The instrumentalization of this approach is also noticeable in the regulatory plane. An illustrative example is the FCC's 2022 decision to ban the use of Chinese-made telecommunications equipment [3]. In parallel, the Cyber Diplomacy Act initiated in 2021 [6] demonstrated Washington's desire to institutionalize its leadership in managing the escalation of cyber conflicts.

Effective response to contemporary challenges requires the consolidation of efforts by democratic alliances. The US promotes norms of responsible state behavior through multilateral platforms such as the UN Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG). Through joint efforts, a normative foundation for global cyber resilience is being formed, based on respect for human rights, openness, and the implementation of internationally recognized technical infrastructure management standards through institutions like ARIN and ICANN.

Conclusions

Summarizing the above, it can be argued that the evolution of US cybersecurity policy demonstrates a logical transition from purely technological dominance (starting from the ARPANET era) to the comprehensive normative and institutional structuring of global cyberspace. The extensive architecture of specialized agencies (FCC, CISA, NTIA) and an adaptive legislative framework testify to the deep securitization of the digital environment, which is today considered not just a communication infrastructure, but a key domain for ensuring national security.

In this context, cyber diplomacy is definitively transforming into a full-fledged strategic narrative arena. Advanced institutional capabilities allow the United States to use the diplomatic attribution of cyber incidents not only as a mechanism of legal responsibility but also as a proactive instrument of strategic communications in the conditions of cognitive confrontation. The ability to publicly identify and expose the subversive activities of non-state actors—transnational media structures or hacker proxy groups—becomes a critical advantage in the struggle for dominance in the information and digital dimension.

Ultimately, the US desire to institutionalize its leadership through multilateral formats (particularly under the auspices of the UN) is aimed at consolidating the global normative order. The consolidation of democratic alliances, the promotion of unified technical standards, and norms of responsible state behavior in cyberspace are necessary prerequisites for ensuring the resilience of institutions in the face of modern hybrid cyber threats.

References

1. About NTIA | National Telecommunications and Information Administration. Home Page | National Telecommunications and Information Administration. URL: https://www.ntia.gov/page/about-ntia
2. About the FCC. Federal Communications Commission. URL: https://www.fcc.gov/about/overview
3. FCC Releases Open Internet Order. Federal Communications Commission | The United States of America. URL: https://www.fcc.gov/document/fcc-releases-open-internet-order
4. The Digital Millennium Copyright Act (DMCA) : PUBLIC LAW of 28.10.1998 no. 105–304. URL: https://www.govinfo.gov/content/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf
5. Hanna K. T. What is the Cybersecurity Information Sharing Act (CISA)?. WhatIs. URL: https://www.techtarget.com/whatis/definition/Cybersecurity-Information-Sharing-Act-
Cyber Diplomacy Act of 2021 : Public Law of 22.04.2021 no. H.R. 1251. URL: https://www.govtrack.us/congress/bills/117/hr1251/text#google_vignette