



CENTRE FOR
JOINT WARFARE
STUDIES

GL/34/24

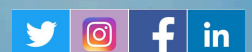
THE RISING RELEVANCE OF INTERNET GOVERNANCE

BY

DR MONOJIT DAS, SENIOR FELLOW, CENJOWS

ORGANISED BY CENJOWS
26TH DEC 2024

WWW.CENJOWS.IN



**THE RISING RELEVANCE OF INTERNET GOVERNANCE
BY DR MONOJIT DAS, SENIOR FELLOW, CENJOWS
ORGANISED BY CENJOWS ON 26TH DECEMBER 2024**

The recent US election, resulting in Donald Trump's re-election as President, has ushered in significant shifts in internet governance. With the creation of a new Department of Government Efficiency led by high-profile appointees, including Elon Musk, global stakeholders must reassess the evolving dynamics between corporate influence, government regulations, and international collaborations. This talk explored the implications of these developments for internet governance, focusing on the challenges posed to multi-stakeholder models, international regulatory frameworks, and global stability.

Multi-Stakeholder Governance: A Changing Dynamics

The multi-stakeholder model of internet governance, encompassing governments, corporations, civil society, and technical experts, faces a special challenge at this juncture. The Vice President-elect's recent threats to European governments over potential bans on Elon Musk highlight an emerging trend: the intertwining of corporate power with state apparatus. This alignment disrupts the balance of the multi-stakeholder approach, favouring corporate agendas. Europe's General Data Protection Regulation (GDPR), often hailed as the gold standard for data privacy, now faces challenges from an administration that prioritizes deregulation and corporate growth. The potential clash between GDPR and the US-driven vision of internet governance could lead to fragmentation, jeopardizing international collaboration on privacy and security.

Corporate and Government Power Play

With Elon Musk's involvement in internet governance, the role of private corporations in critical infrastructure is set to expand. Companies like SpaceX, through initiatives such as Starlink, have already reshaped global connectivity. While these low Earth orbit (LEO) satellites provide internet access to remote areas, they also present challenges to include:

- **Government Dependence on Private Actors:** Increased reliance on private networks could undermine governmental control over internet infrastructure, particularly in areas requiring strategic autonomy.
- **Escalation Risks:** Starlink's dominance in LEO has drawn criticism for overcrowding space, interfering with other nations' satellites, and escalating geopolitical tensions.

European Challenges: Submarine Cable Vulnerabilities

The recent sabotage of Finland's submarine cables, allegedly linked to Russia, underscores vulnerabilities in critical internet infrastructure. Submarine cables carry over 95% of global data, making them vital for internet governance. Such incidents highlight the need for enhanced international cooperation on securing these assets. However, current geopolitical tensions—exacerbated by the US administration's stance—could hinder collective action, leaving global networks at risk.

The Role of Multi-Stakeholder Bodies

Internet governance involves an intricate web of intergovernmental organizations (IGOs), non-governmental organizations (NGOs), civil societies, and academia. The contributions of these actors are central to sustaining an open, secure, and inclusive internet. Some important aspects are as under:

- **UN Internet Governance Forum (IGF):** As the largest global gathering of stakeholders, the IGF has become a critical platform for dialogue. Recent sessions emphasized the need for global cooperation on protecting critical infrastructure, enhancing privacy standards, and addressing emerging technologies like artificial intelligence. However, achieving tangible outcomes has been hindered by disagreements over state versus corporate control.
- **European Dialogue on Internet Governance (EuroDIG):** At the regional level, EuroDIG complements global efforts by tailoring governance discussions to Europe's unique challenges. This year's EuroDIG highlighted tensions between GDPR and external pressures, particularly from the US, and proposed collaborative frameworks to safeguard Europe's digital sovereignty.
- **Civil Society and Academia:** Civil society groups, including advocacy organizations and NGOs, continue to champion equitable internet policies, while academia provides evidence-based research to guide decision-making. Together, they form the bedrock of multi-stakeholder governance, offering diverse perspectives that balance governmental and corporate interests.

Environmental and Strategic Concerns with LEO Satellites

The exponential growth of LEO satellites, spearheaded by companies like SpaceX, poses serious environmental and strategic challenges. Some of these are:

- **Space Debris:** The proliferation of satellites increases the risk of collisions, potentially endangering existing satellites and creating long-term debris problems.

- **Astronomical Disruptions:** The reflective nature of LEO satellites interferes with scientific observations, affecting research and exploration.
- **Escalatory Risks:** The militarization of LEO, driven by private and state actors, risks turning space into a theater of conflict.

The Way Forward

Internet governance post-2024 must reconcile competing interests to ensure stability and inclusivity. Key considerations include:

- Strengthening the multi-stakeholder model by rebalancing corporate and governmental power.
- Enhancing international collaboration to protect critical infrastructure like submarine cables.
- Developing frameworks to manage the environmental and strategic impacts of LEO satellites.