NEXT IAS

DAILY EDITORIAL ANALYSIS

TOPIC

Disinformation, AI, and the Digital Battlefield

DISINFORMATION, AI, AND THE DIGITAL BATTLEFIELD

Context

- The expanding horizons of disinformation, ever-evolving landscape of cyber threats, Artificial Intelligence (AI) and its different manifestations, including Generative AI and Artificial General Intelligence (AGI) create new waves of security threats and concerns over the security specialists the world over.

About

- The year 2024 arrived with a sense of foreboding—a harbinger of new security threats that would test the resilience of nations and organisations worldwide. Among these threats, **two stood out prominently**: the **rise of AI and the expanding horizons of disinformation campaigns**. Together, they wove a complex web—a **'Cyber Chakravyuh'**—that security experts grappled with.

Rise of Generative AI in Disinformation

- Artificial Intelligence, in its various forms, has become both a **boon and a bane. Generative AI and Artificial General Intelligence (AGI)** promise incredible advancements, but they also **open Pandora's box.**
  - **Spreading disinformation** has become disturbingly easy with AI. **Deep fakes**—digitally manipulated videos, audios, or images—now flood our digital landscape.
  - These deceptive creations blur the line between reality and fabrication, causing confusion and chaos. The truth often emerges only after the damage is done.
- In recent years, generative AI has turbocharged state efforts **to manipulate public opinion and suppress dissent**. Governments and political actors worldwide, regardless of their democratic or autocratic leanings, have harnessed AI to create and disseminate deceptive content.
- **Accessibility and Affordability:** Generative AI tools have become more accessible and affordable. This democratisation of technology lowers the barrier for entry into disinformation campaigns.
  - No longer the exclusive domain of well-funded state actors, these tools are now within reach for various entities, including non-state actors and even individuals.
- **Automated Censorship:** AI enables governments to conduct more precise and subtle forms of online censorship. Automated systems can swiftly identify and suppress critical content, making it harder for dissenting voices to be heard.
  - As a result, internet freedom has declined globally, with the 2023 Freedom on the Net report highlighting the 13th consecutive year of such decline.
- **Deep Fakes and Manipulated Content:** AI-generated deep fakes—realistic but fabricated videos or images—have been used to spread disinformation. For instance:
  - **Venezuelan** state media used AI-generated videos of nonexistent news anchors to promote pro-government narratives.
  - In the **United States,** manipulated videos and images of political leaders have circulated on social media, further blurring the line between truth and fiction.
- **Old Tactics Persist:** While generative AI is a powerful tool, governments continue to employ older tactics. A combination of human and bot campaigns is still effective in shaping online discussions.
  - In 2023, at least 47 governments deployed commentators to spread propaganda, doubling the number from a decade ago.

AI's Role in Defense and Deception

- Beyond disinformation campaigns, AI plays a critical role in defence and warfare.
- **Battlefield Deception:** AI can be weaponized for battlefield deception. To counter this threat, advanced AI-based detection tools are essential.

    - Machine learning algorithms can identify patterns indicative of AI-generated deception, preempting cyberattacks or disinformation campaigns.
- **Nonstate Actors and AI:** The use of AI-enabled technologies by both state and nonstate actors offers important insights. Drones, cyberspace, and large-scale mis- and disinformation campaigns all fall within this purview.

Case Studies

- **Taiwan Elections and the Disinformation Storm:** In early 2024, as Taiwan prepared for its elections, disinformation was already rampant. Fake posts and manipulated videos swirled around, creating an atmosphere of uncertainty. While some attributed this to China, the reality was murkier.
    - AI-powered disinformation campaigns had found fertile ground. The cloak of authenticity made it harder to discern fact from fiction. As we navigate this digital age, we must recognize that disinformation, fueled by AI, poses a significant threat to our societies.
- **Ukrainian Conflict:** Ukraine serves as a stark case study. In the ongoing conflict, both sides employ disinformation—including AI-enabled disruption—against each other. The consequences are dire. Misleading narratives, fabricated evidence, and manipulated media fan the flames of discord.
    - The digital battlefield amplifies the physical one, and truth becomes elusive. It's a cautionary tale for the world: disinformation, when combined with AI, can wreak havoc on stability and security.
- **Eternal Vigilance:** The **33rd Summer Olympic Games** in France, held during July-August 2024, were a prime target for digital attacks. Security experts braced themselves for unprecedented threats. Fortunately, the Games concluded without major incidents, a testament to their vigilance.
    - But complacency is not an option. Newer variations of digital threats will emerge, demanding constant watchfulness. National security hangs in the balance, and our defences must adapt accordingly.

A Preview of Cyber Chaos

- Recently, the world witnessed a glimpse of what could unfold during a massive cyberattack. Although not a deliberate attack, a software glitch related to a **Microsoft Windows update** caused a widespread outage.
    - Initially affecting parts of the United States, the glitch quickly spread globally, including India. Flight operations, air traffic control, stock exchanges, and other critical services were disrupted. The **Indian Computer Emergency Response Team (CERT-IN)** classified it as a **"critical"** incident.
- **WannaCry Ransomware (2017):** Infected over 230,000 computers in 150 countries; Resulted in billions of dollars in damages.
- **Shamoon Computer Virus (2017):** Targeted oil companies like SA ARAMCO (Saudi Arabia) and RasGas (Qatar); Labelled the 'biggest hack in history'; Demonstrated the potential impact on critical infrastructure.
- **Petya Malware (2017):** Severely affected banks, electricity grids, and institutions across Europe, the UK, the US, and Australia; Highlighted the interconnectedness of global systems.
- **Stuxnet (2010):** A state-sponsored worm targeting Iran's nuclear program; Physically degraded over 200,000 computers; Showcased the power of targeted cyber weapons.

Related Global Efforts

- **Cybersecurity and Infrastructure Security Agency (CISA):** It plays a critical role in strengthening global cybersecurity. Their international strategy, "CISA Global," focuses on several key areas:
    - **Operational Cooperation:** Collaborating with like-minded partners to share best practices, engage in information exchanges, and issue joint products for global distribution.
    - **Capacity Building:** Building both U.S. and global capacity to defend against cyber incidents and enhance critical infrastructure security.
    - **Stakeholder Engagement:** Strengthening collaboration through outreach and engagement with various stakeholders.

    - **Policy Advocacy:** Shaping the global policy ecosystem to enhance cyber and infrastructure security.
- **Global Collaborations and Norms:** Beyond specific agencies, international organisations like the **World Economic Forum (WEF)** also contribute to global cybersecurity efforts. The WEF hosts discussions, shares best practices, and encourages cooperation among governments, businesses, and civil society.
    - Norms of responsible behaviour in cyberspace are being developed globally. These norms aim to establish guidelines for state behaviour in the digital realm, emphasising responsible conduct and deterring malicious actions.

Related India's Efforts

- **Indian Cyber Crime Coordination Centre (I4C):** The Ministry of Home Affairs (MHA) established the **Indian Cyber Crime Coordination Centre (I4C)** to provide a framework and ecosystem for **law enforcement agencies (LEAs)** to deal with cybercrimes comprehensively and in a coordinated manner.
    - The I4C plays a crucial role in preventing and investigating cyber offences.
- **Indian Computer Emergency Response Team (CERT-In):** CERT-In is the national nodal agency responsible for coordinating responses to cybersecurity incidents, providing early warning and advisories, and promoting cybersecurity awareness and capacity building initiatives across various sectors.
- **Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre):** Launched by CERT-In, the Cyber Swachhta Kendra aims to detect and remove botnets and malware infections from computers and devices across the country.
    - It provides free tools and services to users for securing their systems against cyber threats.

- **Improving Cyber Forensic Facilities:** The government recognizes the importance of robust cyber forensic capabilities. Investments have been made to improve forensic facilities, which aid in analysing digital evidence during investigations.

Conclusion and Way Forward

- As AI continues to evolve, so does its impact on information warfare. While it presents challenges, it also offers opportunities for scalable solutions. Striking the right balance—leveraging AI for societal benefit while safeguarding against its misuse—is crucial in this digital battlefield.
- Our interconnected world demands coordinated efforts to safeguard truth, trust, and stability. And remember, even in the digital realm, eternal vigilance remains the price we pay for safety.
- It is crucial to be informed, vigilant, and collaborative to navigate this 'Cyber Chakravyuh' by **strengthening cybersecurity measures**, and fostering **international cooperation against cyber threats**.

Source: TH

■■■■

Mains Practice Question

[Q] To what extent do you think the increasing sophistication of Artificial Intelligence (AI) is exacerbating the spread of disinformation, and how effectively can governments and societies counter this growing threat?