

## **The Rise Artificial Intelligence and Cyber Defence**

### **What is the issue?**

\n\n

\n

- The rapid commercial diffusion of advanced technologies like artificial intelligence (AI) has been a critical feature of 2017.

\n

- Alongside, the fear that these technologies might pose an unprecedented threat to the future of humanity has also risen.

\n

\n\n

### **What is the current scenario in AI regulations?**

\n\n

\n

- In this era of rapid technological upheavels, the need for greater cyber regulations has been deeply felt.

\n

- A new set of international norms or “a cyber code of conduct” to better protect individuals, companies and nations is already doing the rounds.

\n

- Scientists and entrepreneurs such as Stephen Hawking and Elon Musk, have demanded that the United Nations ban killer robots (AI weapons).

\n

- But while collective agreements within and among nations are far away, the technological advance is likely to be relentless in 2018 and beyond.

\n

- Also, even as calls for preventing the militarisation of AI get louder, governments are relentlessly working to find and exploit new technologies.

\n

- Beyond mere physical threats, AI has the potential to disrupt established services and communication networks, and ideologically indoctrinate masses.

\n

\n\n

## What are Influence Campaigns and Information Weaponisation?

\n\n

\n

- While cyber threats to critical infrastructure has been known for a while, 2017 upended and highlighted its potential for psychological warfare.

\n

- “Influence campaigns” are ones that use AI aided marketing techniques to target individuals based upon their activities, interests, opinions, and values.

\n

- While such campaigns are largely employed for advertising and legal businesses, the allegations of Russian meddling into the US elections have highlighted its potential as a powerful political tool.

\n

- Sophisticated cyber campaigns can hence potentially influence public opinion by blending covert intelligence operations, state-funded media, third-party intermediaries, and paid social media users.

\n

- Such trends have been broadly called “weaponising information” as it is employed to attack the values and institutions that underpin free societies.

\n

- Also, Non-state actors too can employ these tools to wage ideological campaigns to establish and legitimise their narrative of hate.

\n

\n\n

## What is “Information Statecraft”?

\n\n

\n

- As the offensive use of the web has grown, some states have recognized the potential of cyber space and are building capabilities in this sphere.

\n

- **Defence** - China’s great internet wall is one such example, which combines data and the use of AI to rate the loyalty of its citizens to the state.

\n

- Russia has been talking about building an entirely alternative internet to the current one as it feels that it is very American centric.

\n

- Effectively, these are ways to limit and control internet access to domestic audiences for enhancing cyber defence.

\n

- But these programs have become excessively intrusive and undermined individual autonomy and enhance state authoritarianism.

- \n
- Ironically, a few years ago, it was widely assumed that the internet would favour open societies and democracies and undermine authoritarian regimes.
- \n
- **Offense** - Significantly, these countries are also building offensive capabilities to be able to conduct covert and overt cyber operations to influence outcomes.
- \n
- Disinformation and deception has been part of statecraft throughout history and has been employed to undermine enemy governments and societies.
- \n
- But the current trend, which is dubbed as “Information Statecraft”, stands out due to the expansive reach of the social media and the immense potential of big data.
- \n

\n\n

## What does India fare?

\n\n

- \n
- India is a highly diverse society that inhabits a chaotic democratic setup, which naturally makes it very vulnerable to hostile cyber operations.
- \n
- The fact that there is a massive and conscious push by the government towards digitisation makes this all the more significant.
- \n
- The government has actively been seeking to access massive data on citizens for ensuring better tax revenues and services delivery.
- \n
- But there is no public evidence of a coherent strategy for the strategic use of information for internal and external security.
- \n
- Delhi needs to turn its attention in 2018 to creating significant domestic capabilities for information operations against threats at home and abroad.
- \n
- As many state cyber programs have proved abusive, care should be taken to ensure that India’s designs are in full consonance with the rights of its citizens.
- \n

\n\n

\n\n

**Source: Indian Express**

\n\n

\n

