Role of Media and Social Networking Sites in Internal Security Challenges
1. Media ........................................................................................................................................ 2
  1.1. Introduction .......................................................................................................................... 2
  1.2. Role of Media in India .......................................................................................................... 3
  1.3. National Security & Media .................................................................................................. 3
  1.4. Existing Regulations and Restrictions ............................................................................... 5
  1.5. Measures to tackle the threat ............................................................................................ 6

2. Social Media ........................................................................................................................... 10
  2.1. Introduction ......................................................................................................................... 10
  2.2. Social Media vs Social Networking .................................................................................... 10
  2.3. Types of Social Media ......................................................................................................... 11
  2.4. National Security & Social Media ...................................................................................... 11
  2.5. Threat to Internal Security .................................................................................................. 13
  2.6. Key Issues .......................................................................................................................... 14
    2.6.1. Digital Media Regulation .............................................................................................. 14
    2.6.2. Media Trials .................................................................................................................. 16
    2.6.3. Data Localisation .......................................................................................................... 16
  2.7. Available Checks and Balances: Regulations .................................................................... 18
  2.8. Measures to Tackle the Threat ............................................................................................ 19

3. UPSC Mains Previous Years’ Questions ............................................................................. 21

4. Vision IAS Mains Previous Years’ Questions ..................................................................... 22
1. Media

1.1. Introduction

Any communication channel through which any kind of information, news, entertainment, education, data, promotional messages etc. can be disseminated is called media.

Mass media refers to communication devices, which can be used to communicate and interact with a large number of audiences in different languages. Be it the pictorial messages of the early ages, or the high-technology media that are available today, mass media has become an inseparable part of our lives. Media can be broadly classified as:

- **Print Media** (newspapers, magazines, books and Brochures, Billboards, etc.).
- **Electronic Media** (news websites, social networking sites, mass SMS schemes, television, radio, cinema etc.).
- **New Age Media** (Mobile Phones, Computers, Internet, Electronic Books).
1.2. Role of Media in India

For a country like India, the backbone of its democracy and the propagator of its national interests remains the access to information and expression. It helps citizens to make responsible and objective choices, to promote accountability in its officials, to provide solutions for conflict resolution, and to also encourage diverse views of different people. This access to information has allowed the Indian media to play the role of *watchdog*, holding the government accountable in all its activities, and also functioning as a medium for expression for the ordinary citizens.

The role of media in a democracy like India, therefore, can be summed up as:

- **Media as an instrument of expression**: Media in exercise of freedom of expression is essential to communicate the thoughts, views, philosophy, ideals and activities.

- **Media as the Fourth Estate**: It acts as the bridge between the three institutions of the government (Legislature, executive and judiciary) and the people.

- **Educating people through media**: This is largely done by reporting of the news as well as the social commentary on these events.

- **Mass Media can also help in bringing change**: It can be instrumental in bringing about changes in the attitudes and habits of the masses. For example, dispelling the false notions around people suffering from diseases like leprosy, HIV/AIDS, Corona, etc. has been possible only through wide media campaigns.

- **Media promoting distribution of goods**: It drives the consumer choice and generates demand for goods and services through advertisements.

- **Role of Media in Nation Building**: It can aid public involvement through advocating issues of national importance and transferring knowledge, skills and technologies to the people. Awareness about various rural development programs, propagation of family planning could be spread by using the media.

- **Shape the perceptions** of government, influence public opinion, promote democracy, good governance as well as influence peoples’ behavior and support people- oriented policies.

Following the globalization, the responsibilities of media have also widened. It has a role in preserving and pursuing the national interests of the state and highlighting its perspective along with the global issues. It has to examine the status of international relations and again to highlight the trouble spot at global level in lieu of global security.

1.3. National Security & Media

The media and national security policy of a nation have a strong connection in the contemporary environment. Television news in India, with far too many channels competes for viewership 24/7, and with the 'Breaking News' sensation, sets the pace for the print media. The distinction between facts, opinions, and speculation has blurred into irrelevance.

The connection between the media and national security policy is both direct and indirect. The perennial war of ratings of the TV channels has led the newspapers to try to outdo their visual media competitors in order to gain readership. Consequently, newspapers and TV channels report news in a manner that instigates outrage rather than increase awareness and initiate a debate. The threats posed by the media to the internal security include:
The electronic media in particular has long since dropped the pretension of providing a public service, with sensationalisation of every news item without any verification of substance.

Indian media is in no mood to apply brakes or observe self-restraint on its wayward and insensitive treatment of national security issues.

Indian media’s (especially electronic media) analysis of national security issues by groups of former diplomats, generals and academia’s arm chair strategists distorts national security perspectives. All these gentlemen can only draw on their outdated experience and none of them are privy to latest inputs. Also in many cases, reticence is their first casualty after retirement.

Indian TV anchors discussing national security issues do not have the political and strategic maturity to discuss national security issues as their Western counter-parts do.

Indian TV debates on national security issues tend to cut out development of contrary views and perspectives by imposing commercial breaks, or go hectoring themselves.

The role of the media threatens national security when it obtains “unauthorized disclosures leaks” from officials inside the government, and decides to publish or broadcast it, without considering the security implications.

The cut throat competition, especially in case of electronic media, has resulted in priority to exclusivity of coverage over authenticity of the news itself. This manifests in a lack of culture of fact-checking, resulting in dissemination of fake news, often having internal security implications.

The media can also play a negative role in flaming communal tensions through their coverage of various issues. For example, the SC had to intervene to impose a pre-telecast ban on a programme “UPSCJIhad”, partially aired on a news channel.
The rights and responsibilities of the media are not directly enshrined in the written Constitution; however, Article 19 of the Indian Constitution dealing with the freedom of speech and expression broadly highlights the powers and functions of the media as a body of information.

Articles 105(2) and 194(2) allow the Indian Press to publish or report the proceedings of the parliament and the state legislatures.

A number of press laws such as the Press Council Act of 1978 that nominates bodies to govern press functioning in India and the National Security Act of 1980 puts restrictions on the Indian press while reporting on issues that may need to be confidential and whose exposure may threaten the stability of the nation.

The Press Council of India aims to preserve the freedom of the press and maintain and improve the standards of newspapers and news agencies in India. It has the power to receive complaints of violation of the journalistic ethics, or professional misconduct by an editor or journalist.

The Government has been able to restrict the media during emergencies and has imposed laws that diminish its freedom in a limited manner mainly to deal with national security related issues. Some examples include:

- **Defence of India Act, 1962** – It came into force during the Emergency declared in 1962 – the Sino India war. This Act aimed at restricting the Freedom of the Press to a large extent and in turn empowered the Central Government to issue rules with regard to prohibition of publication or communication which would undermine or threaten civil defence/military operations, and also prevent prejudicial reports and prohibition of printing or publishing any matter in any newspaper that may contain such content.

- **Civil Defence Act, 1968** – It allows the Government to make rules for the prohibition of printing and publication of any book, newspaper or other document damaging to the civil defence of the country and its people.

SC on media coverage of social issues.
- The media cannot make a religious minority the target of its attacks. The dignity of a community is as important as journalistic freedom.
- There is a need to strengthen the self-regulatory mechanism by the government in the media.

SC on Censorship of Content
- The general public interest supersedes the requirement to protect the individuality and expression of any artists
- A specific standard of censorship is required to be formulated in this regard to not curb the growth of an artist’s individuality and freedom of expression.
The Broadcasting Code – It was adopted by the Fourth Asian Broadcasting Conference in 1962, highlighting major principles to be followed by the electronic media. The Broadcast Code was set up to govern the All India Radio, but the following key principles have also been followed by all Indian Broadcasting Organizations. The principles include:

- Ensuring the objective presentation of news and fair and unbiased comment, to promote the advancement of education and culture.
- Raising and maintain high standards of decency and decorum in all programmes.
- Providing programmes for the young which, by variety and content, will inculcate the principles of good citizenship.
- Promoting communal harmony, religious tolerance and international understanding.
- Treating controversial public issues in an impartial and dispassionate manner.
- Respecting human rights and dignity.

News Broadcasting Standards Authority - It is an independent body set up by the News Broadcasters Association. Its task is to consider and adjudicate upon complaints about broadcasts.

The Indian Broadcasting Foundation has also released 'Self-Regulatory Content Guidelines for Non-News and Current Affairs Television Channels', after the critical broadcasting of the Mumbai terror attacks in 2008 that brought in media experts and journalists to review the coverage and revise the content of the Indian media.

1.5 Measures to tackle the threat

Considering the potential of media to harm the national security and health of a nation, following measures shall be undertaken to tackle the national threat:

Accuracy in reporting:

- It is the responsibility of TV news channels to keep accuracy and balance, as precedence over speed as usually expected.
- If despite this there are errors, channels should be transparent about them. Errors must be corrected promptly and clearly.
- Channels should also strive not to broadcast which is defamatory or libelous.

India’s National Security Issues and Indian Media Record:

- **India’s Nuclear Weapons TEST 1998**: The Indian media went berserk in politicising the issue. It chimed that there were no national security threats in evidence justifying it. Within seven months the Kargil War took place.

- **Pakistani Proxy War in J&K**: The media has been totally irresponsible. India’s strategic sensitivities are constantly ignored and there is competition to adopt extreme liberalist views. One theme often stressed is of Kashmiri alienation. Had that been so, Pakistan by now would have inflicted a Bangladesh on India.
Kargil War: Instead of marshalling the nation into a cohesive force, the Indian media playing partisan political roles at the height of the war, were busy stoking controversies as to how it happened.

Agra Summit: The summit had more to do with India’s national security interests than political diplomacy. The Indian Media went berserk in focusing and projecting General Musharraf’s view point than advancing India’s interests. What a comparison to the Pakistani journalists who utilised India’s electronic media space to defend and advance their country’s interests.

India’s Military Mobilisation December 2001: Pakistan did not have to use ISI to spy on India’s mobilisation efforts and moves of its strategic formations. The Indian media was doing the job.

Neutrality, Impartiality and Objectivity

- Media must provide for neutrality by offering equality for all affected parties, layers and actors in any dispute, or conflict to present their point of view.

- Though neutrality does not always come down to giving equal space to all sides news channels must strive to ensure that allegations are not portrayed as fact and charges are not conveyed as an act of guilt.

To ensure crime and violence are not glorified

- News channels should exercise restraint to ensure that any report or visuals broadcast do not induce, glorify, incite, or positively depict violence and its perpetrators, regardless of ideology or context.

- Specific care must be taken not to broadcast visuals that can be prejudicial or inflammatory. Equally, in the reporting of violence, the act of violence must not be glamorized, because it may have a misleading or desensitizing impact on viewers.

- News channels must ensure that no woman or juvenile, who is a victim of sexual violence, aggression, trauma, or has been a witness to the same is shown in television without due effort taken to conceal the identity.

- In reporting all cases of sexual assault, or instances where the personal character or privacy of women is concerned, their names, pictures and other details shall not be broadcast/divulged.

Privacy

- As a rule, channels must not intrude on private lives, or personal affairs of individuals, unless there is a clearly established larger and identifiable public interest for such a broadcast.

- However, it is also understood that the pursuit of the truth and the news is not possible through the predetermined principle of prior permission; hence door stepping individuals or authorities for the purpose of news gathering may be used only in the larger purpose of public interest.

- Further, in the case of minors, in any broadcast that intrudes on their privacy, the channel should attempt, where possible, to seek the consent of the parent or legal guardian.
National security

- In the use of any terminology or maps, that represents India and Indian strategic interests, all news channels shall use specific terminology and maps mandated by law and Indian governments.

- News channels shall also refrain from allowing broadcasts that encourage secessionist groups and interests, or reveal information that endanger lives and national security.

- However, it is in the public interest to broadcast instances of breach of national security and loopholes in national security and reporting these cannot be confused with endangering national security.

Superstition and occultism

- News channels shall not broadcast any material that glorifies superstition and occultism in any manner:

  - In broadcasting any news about such genre, news channels will also issue public disclaimers to ensure that viewers are not misled into believing or emulating such beliefs and activity.

  - Therefore, news channels shall not broadcast "as fact" myths about "supernatural" acts, apparitions and ghosts, personal or social deviations or deviant behavior and recreations of the same.

Sting operations

- As a guiding principle, sting and under-cover operations should be a last resort of news channels in an attempt to give the viewer comprehensive coverage of any news story.

- News channels shall not allow sex and sleaze as a means to carry out sting operations, the use of narcotics and psychotropic substances or any act of violence, intimidation, or discrimination as a justifiable means in the recording of any sting operation.

- News channels will as a ground rule, ensure that sting operations are carried out only as a tool for getting conclusive evidence of wrong doing or criminality, and that there is no deliberate alteration of visuals, or editing, or interposing done with the raw footage in a way that it also alters, or misrepresents the truth or presents only a portion of truth.

Strengthening of Institutional Framework

- Giving Press Council of India powers to enforce its guidelines and to penalize newspapers, news agencies, editors, etc. for the violation of its guidelines.

- Government should consider granting statutory status to the News Broadcasters Association (NBA) which represents the private television news and current affairs broadcasters.

- Need for an independent industry led body to enforce core principles of media ethics like truth and accuracy, transparency, fairness and impartiality etc on a regular basis. The body should have powers to impose immediate financial costs for broadcasters and editors in case of violation of these principles.

- Media Trials: In a criminal trial, the prosecution and the accused have the right to a fair trial. Between free speech and fair trial, the borders are sometimes crossed and the rules breached, leading to devastating consequences to individuals and institutions. The 'tele-terror' should not be allowed to meddle with a trial in accordance with the law. The digital violence in itself is a breach of peace.
“The internet is the largest experiment involving anarchy in history. (...) It is a source for tremendous good and potentially dreadful evil, and we are only just beginning to witness its impact on the world stage.”

- Eric Schmidt, Executive Chairman, Google and Jared Cohen, Director, Google Ideas
2. Social Media

2.1. Introduction

Social media is best understood as a group of new kind of online media, which share most or all of the following characteristics:

- **Participation:** Social media encourages contribution and feedback from everyone who is interested. It blurs the line between media and audience.

- **Openness:** Most social media services are open to feedback and participation. They encourage voting, comments and the sharing of information. There are rarely any barriers to accessing and making use of content, password-protected content is frowned on.

- **Conversation:** Whereas traditional media is about “broadcast” (content transmitted or distributed to an audience) social media is better seen as a two-way conversation.

- **Community:** Social media allows communities to form quickly and communicate effectively, sharing common interests.

- **Connectedness:** Most kinds of social media thrive on their connectedness, making use of links to other sites, resources and people.

2.2 Social Media vs Social Networking

Social Media and Social Networks in actual terms differ as social media is a communication channel that transmits information to a wide audience and is usually a one-way street, while social networks facilitate the act of engagement between like-minded people, groups or communities.
2.3 Types of Social Media

There are several kinds of social media:

- **Social networks:** These sites allow people to build personal web pages and then connect with friends to share content and communication.

- **Blogs:** a blog is an online journal where the entries are written in a personal, conversational style. They are usually the work of an identified author or group of authors.

- **Wikis:** These websites allow people to add content to or edit the information on them, acting as a community document or database. Example - Wikipedia

- **Forums:** Areas for online discussion, often around specific topics and interests. Each discussion in a forum is known as a 'thread', and many different threads can be active simultaneously. This makes forums good places to find and engage in a variety of detailed discussions. **One major difference between forums and blogs** is that the Blogs have a clear owner, whereas a forum’s threads are started by its members.

- **Content communities:** They organize and share particular kinds of content. Here, you have to register, get a home page and then make connections with friends. The most popular content communities tend to form around photos (Flickr), bookmarked links (del.icio.us) and videos (YouTube).

- **Micro-blogging:** Social networking where small amounts of content (updates) are distributed online and through the mobile phone network. Example- Twitter

2.4 National Security & Social Media

Social Media can represent an effective opportunity to preserve national security and/or reach the strategic interests of a state if used properly by civil institutions and, in particular, by security services and/or information security services. Besides, these tools “can be used by governments for content creation, external collaboration, community building, and other applications” and that “failure to adopt these tools may reduce an organization’s relative capabilities over time”.

Security and law enforcement agencies can use social media platforms in the following ways for internal security:

- To use data available freely on social media platforms to gauge the mood of citizens on issues, predict patterns and possible flash points of disturbances, and prevent and react to cyber-crimes.

- To build actionable intelligence which may support human intelligence efforts which could be shared across agencies, with built in safeguards to ensure that there is no encroaching upon the privacy of citizens.

The use of social media for policing may be seen by many initiatives like:

- Delhi Traffic Police using platforms like Facebook and Twitter to ease handling of traffic related issues,
- Delhi police online FIR facility for lost articles,
- Indore police using the medium to track criminal activity
- Bengaluru police twitter handle selected for “Twitter Samvad”.
- Social Media Labs Project by Maharashtra Police tracks activity on social media to anticipate and handle sudden flare ups.
The ability to forestall future strategic and tactical contexts is of paramount importance in order to reduce the possibilities to be caught by surprise by threats and increase the resilience to them.

Warning and Trend Prevision Tool-

- A state has to reach Information Superiority, referred to as an advantage over the adversary in IT and decision-making, if they really want to guarantee high competitiveness and efficiency standards, protect their own strategic interests and effectively counter threats to national security.

- Social Media can help reach this kind of competitive advantage since they increase the agility and flexibility of the information sharing procedures and accelerate the decision-making process.

- to inform and engage with citizens to build secure communities which share information;

- to ensure presence to combat misuse of social platforms to spread malicious rumors which may trigger problems for internal security and law and order, and prepare standard operating procedures for times of emergency;

Institutional Communication Tool-

- The use of Social Media allows not only to communicate, share or capture information, analyze sociopolitical dynamics and anticipate economic-financial trend, but also to describe events, model reality, influence the perception of a certain situation, a specific issue or a person, and influence choices and behaviors. For example, the use of fake social media profiles to influence public opinion towards Presidential candidates by external state actors was witnessed in the 2016 US elections.

Negative Impact of Social Media on Democracy

- Foreign Interference: It has been used as an information weapon to influence public sentiment in elections by external state actors. For ex. the setting up and promotion of fake pages on Facebook by Russian entities in US 2016 election.

- Fake News: It has allowed criminal actors to launch misinformation campaigns and incite violence.

- Echo Chambers: It creates bubble where people only see viewpoints they agree with, strengthening the preferred narratives and rejecting the information that undermines it, thereby creating a polarised society.

- Political Harassment: As more countries write laws that attempt to criminalize online discourse, the risk grows that states use their power to intimidate their critics. That could have a chilling effect on speech.

- Unequal Participation: Vulnerable populations could end up ignored, and fringe groups could appear mainstream.

Influence, Propaganda and Deception Tool-

- Foreign Interference: It has been used as an information weapon to influence public sentiment in elections by external state actors. For ex. the setting up and promotion of fake pages on Facebook by Russian entities in US 2016 election.

- Fake News: It has allowed criminal actors to launch misinformation campaigns and incite violence.

- Echo Chambers: It creates bubble where people only see viewpoints they agree with, strengthening the preferred narratives and rejecting the information that undermines it, thereby creating a polarised society.

- Political Harassment: As more countries write laws that attempt to criminalize online discourse, the risk grows that states use their power to intimidate their critics. That could have a chilling effect on speech.

- Unequal Participation: Vulnerable populations could end up ignored, and fringe groups could appear mainstream.
2.5 Threat to Internal Security

Social media poses challenge for democracies because the channels such as social networks and blogs present powerful tools to spread information to the masses. Few examples to remember are the Moldavian twitter riot, the London riots, the Iran elections, the WikiLeaks disclosures, or the Arab freedom movements. The efficient use of the tools provided by the new media is the new military power because electronic media and social media are the most effective and powerful means of mass motivation.

For the Indian government, the internet remains the chosen platform for socio-economic empowerment schemes, which also makes India uniquely dependent on internet platforms for its development while, at the same time, it heightens the risks of India's vulnerabilities.

Terrorism:
- Social Media are more and more used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training.
- The rapid expansion and development of social media can be used to cause problems by propagating certain ideologies, mobilizing and organizing people.

Protest Movements and Revolution:
- Social Media constitute an asset of great importance both for protest movements and for revolutions. Rebels and revolutionary groups turn to such tools to better organize and spur masses to action, to arrange protest or struggle activities and manage their tactical and operational aspects.
- It has a potential for disrupting public order, either involuntarily through the unchecked spread of rumors, or deliberately through the propagation of misinformation with the intent of creating enmity between groups.
Criminal organizations use Social Media as support, communication and coordination tools to conduct their illicit activities.

This kind of illicit activities can be either purely information ones (i.e. spreading child pornography with fee, “virtual” identity thefts, phishing, spread of viruses, Trojans, worms, etc.), or “traditional” ones (i.e. drug smuggling, human trafficking, money-laundering, transfer of documents from industrial espionage).

Mobile phone technology provides easy and instant digital camera and video facilities, and this can be used maliciously.

Cases of cyber bullying, misuse and corruption of personal information, the posting of material about an individual by third parties, often of a malicious nature, and publishing of material involving others, without their consent, which can be embarrassing or worse.

War:

According to a recent NATO provisional study, future conflicts will occur in more and more connected environments, which will be characterized by the use of new communication and information technologies, Social Media included.

The media networks are regularly hacked by enemy countries to spread false information and to recover classified data. Recently hacking of New York Times and Twitter servers by Syrian agencies was in news. Similarly, the US and China continue to exchange blows in the field of hacking.

Silent circle’s applications: A threat

- Silent Phone: Encrypted voice and video calls on mobile devices. It can be used with Wi-Fi, EDGE, 3G or 4G cellular anywhere in the world.
- Silent Text: Encrypted text messaging with 'burn notice' feature for permanently deleting messages from device registries.

2.6 Key Issues

2.6.1 Digital Media Regulation

Digital Media can be broadly classified into the following:

1. Social Networking Sites like Facebook, and microblogging websites like Twitter etc.

2. Over the top (OTT) platforms

1. Social Media Regulation

Given its characteristics to potentially give “voice to all”, immediate outreach and 24*7 engagement, Social Media offers a unique opportunity to governments to engage with their stakeholders especially citizens in real time to make policy making citizen centric. Many governments across the world as well many government agencies in India are using various social media platforms to reach out to citizens, businesses and experts to seek inputs into policy making, get feedback on service delivery, create community based programmes etc.

However, this has also created its own set of issues like:
1. **Lack of privacy:** Stalking, identity theft, personal attacks, and misuse of information are some of the threats faced by the users of social media.

2. **Cyber bullying:** People can misuse social media platforms to spread rumors, share videos aimed at destroying reputations and to blackmail others.

3. **Fake news:** While everyone becomes a source of information, hardly anyone adheres to the strict standards of scrutiny required for the information to be passed on as news. This results in a barrage of fake news with real life consequences.

4. **Trolling:** According to the Research by Amnesty International,

   - Women are targeted with abuse online not just for their opinions – but also for various identities, such as gender, religion, caste, and marital status.
   - Indian women politicians face substantially higher abuse on Twitter than their counterparts in the U.S. and the U.K.
   - Women from marginalized castes, unmarried women, and those from non-ruling parties faced a disproportionate share of abuse.

5. **Accountability issues - Challenges with respect to fixing the liability of intermediaries.**

6. **Jurisdictional challenges -** Complications in jurisdiction as Facebook etc. operate as subsidiaries of foreign internet companies with their servers located outside India.

7. **Anonymity -** Police officers have expressed concern over multiplicity of fake profiles.

---

**Softer targets**

Women politicians form India faced significantly more abusive and problematic tweets compared with their counterparts in the U.S. and the U.K. Muslim women politicians, in particular, faced more such tweets than others.
2. Over-the-Top Platforms

The Ministry of Information and Broadcasting ("MIB") has been undertaking the ginormous task of regularizing and certifying the content available on various entertainment platforms and digital media in general, more particularly referred to as the over the top platforms ("OTT"). MIB would soon call for talks with the major stakeholders of the prevalent OTTs, including Netflix, Amazon Prime Now, Hotstar etc. as also with members of civil society, technical community, media and legal experts, in order to discuss and formulate a concrete mechanism of certification and regularization of the content available on such OTTs.

This requirement for the MIB to formulate regulations to certify and regularize the content available on OTTs has stemmed from the displeasure of certain groups in relation to certain web series (which are currently being streamed on such OTT platforms) as 'violent' and 'vulgar'. The High Court of Karnataka has also suggested to the Central Government to consider setting up a mechanism of certification and regularisation of the online content.

2.6.2 Media Trials

Media trial describes the impact of television and newspaper coverage on a person’s reputation by creating a perception of guilt irrespective of the verdict in a court of law. There has been no legal system where the media is given the power to try a case. Every coin has two sides so is the case with media trials and journalism, at certain instances journalist portrays a pre-decided image of an accused thereby tearing his/ her reputation that can eventually affect the trial and the judgment, henceforth trial by media.

Famous Examples

There have been quite infamous cases as well that outraged the public and impacted the Judiciary such as The Jessica Lal case (2010) where the media rejoiced over their efforts in bringing justice to Jessica Lal and the trial court had acquitted the accused of all the charges. The PriyadarshiniMattoo case (2006) where a law student was raped and murdered and the judgment of this case was suspected to have been influenced by Media Trial.

There are grounds which make the attention of the media around certain cases high, which include:

1. Cases could involve children or they could be so gruesome that it shakes the collective conscience of the society.
2. Cases involving celebrities either as victims or as accused.

Judges and judicial officers are not free of faults and can be “subconsciously influenced” by media trials or media publicity. Therefore, it becomes necessary to regulate media publicity while the trial is going on or pending.

2.6.3 Data Localisation

What is it?

Data localization is a concept that the personal data of a country’s residents should be processed and stored in that country. It may restrict flow entirely or allow for conditional data sharing or data mirroring (in which only a copy has to be stored in the country).

There is a growing perception that data localization will aid countries asserting sovereignty in digital domain, ensure informational security of its citizens & fare better in governance (as it goes digital).
Need for Data Localisation

- Economic development of the country: Data is the new oil, an economic resource, fueling the 4th Industrial Revolution.
  - Digital data in India to increase from 40,000 PetaByte (PB) in 2010 to 2.3 million PB by 2020 - twice as fast as the global rate. If India houses all this data, it will become 2nd largest investor in the data centre market and 5th largest data centre market by 2050. This will give significant push to AI led economy in India.
  - India has 2nd highest FinTech adoption rate amongst major economies in the world. Data localization would give a push to domestic production of high value digital products.
  - Domains of cloud computing, data analytics etc. can become major job creators in future.
  - There is a push among government department to use AI tools and attempt a predictive approach to policy making. With data localization, there is a scope of greater access to 'public data' collected by companies (e.g. traffic data collected by like Uber, street level data collected by Google Maps) for the Government.

- Increase India’s tax revenue: Extensive data collection & processing by technology companies, and unfettered control of user data has allowed them to freely monetize Indian users’ data outside the country without paying any taxes.
  - Localization would lead to a larger presence of MNC's in India overall, through local offices, and increase tax liability and open more jobs.
  - Data localization is supported by domestic companies like PayTM and PhonePe as it will level the playing field, currently rendered unequal due to differences in tax liabilities of international companies and those having permanent establishment in India. E.g. Google India tax dispute over advertisement revenue under litigation in court.

- Maintain data sovereignty & citizens’ data privacy: With data stored in remote servers, the accountability of service providers (like Google, Facebook etc.) reduces as it is outside the purview of Indian regulatory authorities. With data localization, regulatory oversight on end-use of data will improve and business jurisdiction related loopholes will be plugged. E.g. Facebook shared user data with Cambridge Analytica to influence voting.

- Issue of national security: Data localization will help law enforcement agencies to get access to user data for investigation and prosecution
  - Currently, companies are dependent on Mutual Legal Assistance Treaties (MLATs) to obtain data from US companies leading to delays and legal challenges in foreign jurisdictions.
  - In many countries like US, tech companies are legally barred from disclosing data to foreign law enforcement agencies.

Before universalizing the policy of data localization, the Government needs to provide a push to local capabilities in data storage and processing

- Infrastructure status to data centres/server farms
- Adequate physical infrastructure (energy, real estate and internet connectivity) for setting up such centres

India should put in place a cybersecurity law to ensure protection of private data of citizens.

Measures towards Data Localisation

- In 2018, a draft data protection law by BN Srikrishna Committee also recommended that all personal data of Indians have at least one copy in India. It also defined a category of data as critical personal data, which must be stored and processed only in India.
- A similar clause was incorporated in Government’s draft e-commerce policy, which recommended localization for “community data generated by users in India from various sources including e-commerce platforms, social media, search engines etc.”
The way in which the internet allows data to be produced, collected, combined, shared, stored, and analyzed is constantly changing. Police projects like Social Media Labs depend entirely on information available on public platforms and hence authorities must anticipate contestations to what constitutes public data in times ahead.

The government is working on a policy which is aimed at keeping a hawk’s eye vigil on the social media to check if it is being "misused" to conspire against India and spread anti-national propaganda - a regulatory framework for social media and online content. At present, there is only a set of "do's and don'ts" for the social media which needs to be graduated to a full-fledged guidelines that should be adopted on such a network.

Supreme Court has also expressed its concern for uncharitable comments, trolls and aggressive reactions on social media platforms on almost every issue, including judges and judicial proceedings. As use of social media evolves, for security and law enforcement agencies, questions regarding ‘relevancy’ of such data, and its ‘admissibility’ etc. will also be raised.

Under the existing legal frameworks, Sections 69 and 69(a) of IT Act 2000 empowers the government of India to:

- **Issue directions for blocking of information** for public access and to issue directions for interception or monitoring or decryption of information through any computer resource when circumstances threaten public order, defence, security, sovereignty and integrity of India, or friendly relations with other states or to prevent incitement to the commission of any cognizable offence relating to the above circumstances.

- Article 69 (b) of the IT Act 2000 empowers agencies of the government of India, in this case the Dept. of Electronics and Information Technology, “to authorise to monitor and collect traffic data or information through any computer resource for cyber security” for cyber incidents and breaches.

Draft Information Technology (Intermediary Guidelines) Rules 2018 have increased the responsibilities of the social media platforms to regulate and prohibit users from hosting obscene content on the platform. (Refer Infographic)

### What the Amended Rules Propose

<table>
<thead>
<tr>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cos have to <strong>trace and report origin</strong> of messages within <strong>72 hours</strong> of receiving a complaint from law enforcement agencies.</td>
</tr>
<tr>
<td>Will have to <strong>disable access</strong> within <strong>24 hours</strong> to content deemed defamatory or against national security and under other clauses of Article 19 (2) of the Constitution.</td>
</tr>
<tr>
<td>Such Info and associated records will have to be <strong>preserved for 180 days</strong>.</td>
</tr>
<tr>
<td>Platforms with more than <strong>5m USERS</strong> must have <strong>registered entity</strong> in India under Cos Act.</td>
</tr>
<tr>
<td>They will have to appoint a nodal officer in India to deal with <strong>law enforcement agencies</strong> on a <strong>24X7 basis</strong>.</td>
</tr>
<tr>
<td>Cos also must <strong>send communication to users</strong> <strong>ONCE a month</strong> about their privacy policies.</td>
</tr>
<tr>
<td>Platforms must deploy tools to <strong>identify and remove</strong> or disable public access to unlawful information or content.</td>
</tr>
</tbody>
</table>

---

For detailed enquiry, please call:
+91 8468022022, +91 9019066066
ENQUIRY@VISIONIAS.IN @VISIONIAS

DELHI, JAIPUR, HYDERABAD, PUNE, AHMEDABAD, LUCKNOW, CHANDIGARH, HYDERABAD
2.8. Measures to Tackle the Threat

The nature of the medium is such that it has raised valid questions as to whether regulation is possible without infringing on the fundamental rights of the citizen relating to freedom of speech and privacy. Due to its characteristics, its constituents, its contents and its evolving power, Social Media cannot be controlled, censored or shut down. Social media has to be understood and adopted.

- **Institutionalise the blueprint for a National Social Media Policy:** The National Cyber Security Policy needs to be revised to include social media challenges which are distinct from the cyber security threats.

- **Implement and institutionalise the Framework of Guidelines on social media engagement for the government organisations with the following elements:**
  - Objective: Why an agency needs to use social media
  - Platform: Which platform/s to use for interaction
  - Governance: What are rules of engagement
  - Communication Strategy: How to interact
  - Pilot: How to create and sustain a community
  - Engagement Analysis: Who is talking about what, where and what are the main points of conversations
  - Institutionalisation: How to embed social media in organisation structure

- **Empower agencies, build talent, and use specialists:** If the medium is to be adopted into daily practice by all personnel, then agencies must be empowered technically, legally and financially to use the medium to their specific purposes.

- **Need a code of practice on disinformation:** In line with the code by EU, it should allow platforms and agencies to take action in 5 areas:
  - Disrupting advertising revenues of certain accounts and websites that spread disinformation;
  - Making political advertising and issue based advertising more transparent;
  - Addressing the issue of fake accounts and online bots;
  - Empowering consumers to report disinformation and access different news sources, while improving the visibility and findability of authoritative content;
  - Empowering the research community to monitor online disinformation through privacy-compliant access to the platforms’ data.

- **The authorities can use the same medium to provide correct information and nip rumors in the bud.** Existing technologies and laws provide sufficient leeway to the authorities to effectively monitor internet traffic, including social media, in real-time, but are under-utilized for a variety of reasons, largely to do with coordination.
Social media analysis generated intelligence or SOCMINT is being developed as a successful model in many countries abroad to isolate hotspots or subjects that go viral and is used as a predictive tool. India too is looking at these models, but is still at the stage of experimentation, trial and error.

We need more social media pilot projects across the country to develop a truly credible database and this will require huge investments in terms of both infrastructure and human resource. We also need to work on network availability constraints, language barriers and, most importantly, organizational adaptability in terms of this new medium.

We need to make people aware that the internet is not, in reality, a private place. The citizens should be guided of the advantages and of the risks of social networking sites, and provided an overall awareness, particularly to the young and vulnerable, about the need to be cautious in what they do online.

From a corporate perspective, a revised security model which takes into account the sharing of information across social networks is necessary. There are risks in the use of and social networking software, though these are often not well recognized.

A strengthening of legislation designed to protect personal information.

Working to define and then to protect data ownership rights in a web-based environment.

The unique way that the internet continually improves in response to user experience is driving innovation on an unprecedented scale. Social media is developing in response to the appetite for new ways to communicate and to the increasingly flexible ways to go online. Its future direction is impossible to predict. What is beyond doubt is that social media – however it may be referred to in the future – is a genie that will not be disappearing back in to its bottle.
1. What are social networking sites and what security implications do these sites present? (2013)

2. "The diverse nature of India as a multi-religious and multi-ethnic society is not immune to the impact of radicalism which is seen in her neighbourhood? Discuss along with strategies to be adopted to counter this environment. (2014)

3. Religious indoctrination via social media has resulted in Indian youth joining the ISIS. What is ISIS and its mission? How can ISIS be dangerous to the internal security of our country? (2015)

4. Use of internet and social media by non-state actors for subversive activities is a major security concern. How have these been misused in the recent past? Suggest effective guidelines to curb the above threat. (2016)

5. Mob violence is emerging as a serious law and order problem in India. By giving suitable examples, analyze the causes and consequences of such violence. (2017)
4. Vision IAS Mains Previous Years' Questions

1. The Supreme Court of India on the reckless media coverage of the 26/11 attacks noted that - “By covering the attack live, the Indian TV channels were not serving any national interest or social cause. On the contrary, they were acting in their own commercial interests, putting national security in jeopardy.” In the light of the above observation, mention the principles and concerns that mass media should keep in mind while reporting sensitive and dangerous issues.

Approach:
The concerns indicated should be comprehensive, covering the aspects of impartiality, objectivity, sensitivity, privacy and national security. There is no need to go into a criticism of media in Mumbai terror attacks. The statement is only to highlight the importance of sensitivity in media reporting.

Answer:
Media, due to its power to influence the decisions of others and its role of information, education and communication, is considered as the fourth pillar of democracy. Hence, it becomes necessary that media follows certain principles of self-regulation so that it does not create, intentionally or unintentionally, problems for national security and law and order. Some important principles to be followed by the media are:

1. **Impartiality and objectivity in reporting:** Viewers of 24-hour news channels expect speed but that should not be at the cost of accuracy and balanced reporting. If errors in reporting have been made, they should be promptly admitted and corrected.

2. **Ensuring neutrality:** Equal opportunity must be given to all parties and actors to present their point of view. Neutrality does not mean giving equal space to all sides but it must be ensured that allegations are not portrayed as facts.

3. **No glorification of crime and violence:** Media should exercise restraint to ensure that any report or visual broadcast do not induce or glorify violence. Specific care must be taken not to broadcast visuals that can be inflammatory.

4. **Special care in cases pertaining to women and children:** In reporting cases of sexual assault or other cases involving privacy of women, their personal details should not be divulged. The identity of victims of child abuse and juvenile delinquents should be kept secret.

5. **Refrain from obscenity:** News channels must ensure that they do not show nudity or use sexually selective language.

6. **Respect individual privacy:** Channels must not intrude into personal affairs of individuals unless there is a clearly established larger and identifiable public interest.

7. **Should not endanger national security:** News channel should refrain from allowing broadcasts that encourage secessionist groups and interests. They should not reveal information that endangers lives and national security.
8. **Refrain from sensationalizing:** Media should take care that they do not indulge in sensationalizing news to gain more TRP. Special care is needed in instances of communal violence and sectarian conflicts to ensure that biased and prejudicial reporting is not done.

The Supreme Court’s observation should act as an early warning to the media, which has been blinded by the need for greater audience and TRP. Self-regulation is the best form of regulation, especially in case of media. Hence media should try to stick to above principles so that its freedom remains ensured.

2. “While social networking sites have created a seamless and interconnected platform for communication, they have also created many challenges for our internal security”. Comment.

**Approach:**

Justify the statement in the question in brief, citing how social media has broken down barriers of communication in modern era. Thereafter, one should highlight some of the challenges posed by misuse of social media to internal security. End the answer with a brief description of challenges and steps that should be taken by the government with regards to this problem.

The biggest positive of the social networking sites is that anybody can freely access them and use them for self-expression. Social networking site have reduced the communication barriers among the people. Many organisations are known to use social media strategies to reach out to customers and peers quite successfully. Even the governments have been using social media for broadcasting information about schemes and programmes to a great effect.

While at the same time the biggest danger lies in the possibilities of misuse of these sites from within or across the borders by anyone, either individually or through organized means. These sites are a store house of personal information and mass dispersion of information both; hence, there misuse can pose major security threats.

**Social security sites posed major internal security threats in past**

1. **Misuse of social media sites to ignite communal passions:** Intelligence bureau Chief Asif Ibrahim in 2013 pointed out that misuse of social media to fan communal tensions was the biggest threat to internal security, giving the example of a video that was circulated to incite communal violence in Muzaffarnagar. Hand of Indian Mujahidden was suspected in the same.

2. **It can cause mass panic, confusion and spontaneous reactions through misinformation:** The unprecedented cyber terrorism unleashed against people from North-East triggered big exodus within the country, with the north-eastern people fleeing major areas in Karnataka, Tamil Nadu, Maharashtra. All the sites were found hosting inflammatory and hateful content against people from north east inciting violence against them.

**Why have these sites been able to pose a threat to internal security? The Problems:**

- Proxy servers and virtual private network services which conceal the user identity operating from a number of countries appear to have been used for inciting passions and spreading misinformation.

Google, you-tube, Twitter and Blogspot.com, do not show willingness to share the IP addresses of the users and their information directly who indulge in cyber terrorism. They request the governments to approach them through US government as they function under US IT laws, although India has a mutual legal assistance treaty with them.
Google was more cooperative and any content which could incite violence was already blocked on it, but other sites like twitter refused to remove a major chunk of the inflammatory content, sating that inflammatory content was outside the jurisdiction of the country.

The government finds itself in a new information battlefield with no contingency plan, for the moment. Impulsive reaction was an immediate crackdown but, India has become second highest user of facebook., this is an audience that the government should reach out to, along with keeping a track that no population become victims of cyber-attacks.

3. While social media is being increasingly used to instigate communal riots and create social tensions, any effective strategy to check its misuse must balance security concerns and individual rights. Discuss in the context of recent developments in India.

Approach:

- Introduce answer with commentary on use of social media for creating tension in society.
- Discuss the restriction imposed by government.
- Comment on the Supreme Court judgment on Section 66A of IT Act.
- Suggest measure to balance the individual right and public order.

Answer:

In recent years, the social media has been increasingly used (in India) to instigate communal and social tensions. Law enforcement agencies have witnessed a worrying trend in last few years where social media posts and circulation of doctored audio-visual material over social networking site led to communal incidence.

Riots in Muzaffarnagar, exodus of people from North-East from southern states are some of the events that highlight the threat from social networking sites. Circulation of inflammatory audio-visual material was the prime factor in these incidences.

In response there is tendency among law enforcement agencies to impose additional restrictions on what is said and propagated on the social media. Any strategy to check the misuse of potential threats from the social networking site may lead to curtailment of fundamental rights guaranteed in constitution. Indian government amended the Information Technology Act (IT Act 2000) in 2009 to include section 66A aimed at checking misuse.

However, its blatant misuse led to denying rights essential for healthy democracy. The Supreme Court of India recently passed a judgment declaring the section as unconstitutional. The case highlights the importance of a proper balance between civil liberties, individual human rights, and the responsibility of the state to maintain peace and order.

It is not a simple case of misuse of law. In fact, the law suffers from the vice of non-application of mind. A bare reading of the section reveals how vaguely worded it is. It prescribes a maximum punishment of a prison term of 3 years with fine for sending information that is "grossly offensive" or has "menacing character" and for sending e-mails causing "annoyance or "inconvenience" to the recipient.
However, information technology has been recurrently exploited to harass or create public disorder cannot be denied. Section 66A has proved to be a useful remedy, particularly in situations of sensitive nature concerning religious and communal sentiment; for instance the episode of the exodus of north-east students from Bangalore where the Police Authorities were forced to take recourse to section to avoid spreading of rumours to incite violence against persons of the North Eastern community.

Such instances where religious and communal harmony have been disrupted by publishing/transmitting inflammatory content in the form of texts, mails, posts, etc. have to undoubtedly be deemed as “grossly offensive”.

A multi-racial, multi-cultural country like India, where free speech is susceptible to misuse on sensitive grounds of communal, political and religious bias, needs reasonable restrictions to check misuse. Best way to address the concerns is to come with amendments to the scraped section so that it reduces the discretion in the hands of frontline officers.

We need non-legal initiatives by the government, the media, schools, not-for-profit organizations, religious and caste associations and a slew of other groups to further empower users to deploy such strategies to fight abuse and hate speech over the internet.

4. Monitoring social networking sites, phone tapping etc. are an infringement on the privacy, but need of the hour in wake of the recent domestic scenario. Examine.

Approach:
Examine both the pros and cons of such surveillance programs and offer some practical suggestions on how the concerns of groups on both sides of the divide could be addressed.

Answer:
Given the rising incidences of terrorism and security threats, nations across the world, have been monitoring electronic communications for the purpose of protecting and preserving their sovereignty, integrity and security.

This has come to be seen as inevitable given the use of technology by criminals, terrorists and organized crime syndicates for anti-national activities.

India’s Central Monitoring System (CMS) and the Prism Program of USA are instances of surveillance programs put in place by countries across the world.

It has been argued that in the event of a conflict between national interest and individual liberties, it is the former that shall prevail. Also, the Right to Privacy is subject to reasonable restrictions on various grounds.

The proponents of government surveillance argue that such projects will eventually strengthen the security environment in the country.

The proponents also argue that while in traditional surveillance systems secrecy could be easily compromised due to manual intervention at various stages, this shall be minimized in new systems like the CMS. This is because in CMS, functions will be performed on a secured electronic link and there will be minimum manual intervention.
However, the critics express concern over the sheer lack of public information on such projects. There is hardly any official word from the government about which government bodies or agencies will be able to access the data, how they will use this information, what percentage of population will be under surveillance, or how long the data of a citizen will be kept in the record.

This makes it impossible for citizens to assess whether surveillance is the only, or the best, way in which the stated goal can be achieved. Also, citizens cannot gauge whether these measures are proportionate i.e. they are the most effective means to achieve this aim.

In such projects, often there is also no legal recourse for a citizen whose personal details are being misused or leaked from the central or regional database.

Blanket surveillance techniques, like the CMS, also pose a threat to online business. With all the data going in one central pool, a competitor or a cyber criminal rival can easily tap into private and sensitive information by hacking into the server.

There is also the possibility that as vulnerabilities will be introduced into Internet infrastructure in order to enable surveillance, it will undermine the security of online transactions.

These projects can also undermine the confidentiality of intellectual property especially pre-grant patents and trade secrets. Rights-holders can never be sure if their IPR is being stolen by some government in order to prop up national players.

Civil rights groups also argue that security cannot be prioritized by large-scale invasions of privacy, especially in a country like India where there is little accountability or transparency.

In light of these arguments there is an urgent requirement for a strong legal protection of the right to privacy; for judicial oversight of any surveillance; and for parliamentary or judicial oversight of the agencies, which will do surveillance.

Moreover, an attempt must be made to reach a middle ground between privacy and security - a system, which takes care of national security aspect and yet gains the confidence of the citizens. The secrecy period can be kept restricted to three to four years in such projects. Thereafter who all were snooped and when and why and under whose direction/circumstances must be made public through a website after this time gap.

5. Assess the potential of Social Media Networks for effective policing in India. Also, highlight the reasons behind relatively slow pace of adaptation of social media into policing in India.

Approach:

Write down and assess the potential of social media for effective policing.

Mention the reasons which have led to slow pace of adaptation of social media into policing.

Answer:

The Police departments, globally as well as in India, are increasingly dependent on technology to gather information, create awareness and maintaining a public interface. In this context, social media provides huge potential for policing in India, as millions of Indians are active users of Facebook, Twitter, WhatsApp and other platforms. This can be understood from the following points:
Problem solving in policing requires information exchange, problem identification, problem solving and trust. Social media can help with all these aspects.

Social Media can support policing by increasing citizen participation to identify crime, reducing the communication gap and improve co-ordination between the police and citizens. For e.g. timely reporting of criminal activities by citizens helps in prevention and investigation of crime etc.

Feedback from citizens and understanding their grievances and opinion through social media leads to a holistic development of the police department.

Some social media tools facilitating anonymity help citizens overcome their social fear to complain about issues of law and order.

Social media helps in disseminating information and forewarn citizens about areas that might see a conflict. Police uses Facebook and twitter pages to keep citizens informed about policing arrangements.

Nonetheless, these very factors also put certain limitations and challenges for policing:

Social media has made it possible to spread rumour and create panic in a short span of time.

It has also made the police personnel, even their personal lives, subject to intense scrutiny. Anonymity makes it easier to make frivolous allegations tarnishing the image of a police personnel.

The widespread use of social media also poses a challenge of gathering actionable intelligence through a vast swathe of data.

Overall the potential utility as well as challenges posed by the widespread use of social media makes it imperative that the police adapts to the changing scenario. However, adaptation of social media in policing has been very slow. This is due to the following reasons:

The lack of manpower as well as of technological capabilities of handling social network pages of police inhibits social media adoption for community policing.

Resistance to technology by police departments in some states

Digital illiteracy in general and lack of awareness among people regarding use of social media for policing in particular is an inhibiting factor.

Unclear and generic information from police and violent and abusive content from citizens reduces the efficacy of social media for policing.

An absence of comprehensive policy in many states regarding use of social media in policing.

It is very difficult to segregate genuine complains. Thus, there is a chance to misuse social media to spread rumours.

Concerns regarding data safety and privacy also is becoming a major hurdle in adopting social media in policing

The aim of social media is to achieve decentralized decision-making that empowers field officers to identify crime, prioritizing the problem with the help of local citizens, and introducing transparency in the policing. An efficient social media strategy that focuses on the potential rewards of using social media and mitigating its risks is the
6. Identify the opportunities and challenges that social media presents to the law enforcement agencies in India to counter national security threats. What steps have been taken to address the challenges?

Approach:

- Provide a brief introduction of social media usage in India.
- Mention opportunities and challenges posed by it to the law enforcement agencies in countering national security threats.
- Mention steps taken by the government to address these challenges.
- Conclude with a way forward.

Answer:

With over 500 million active Internet users, social media usage in India is also on the rise. In this context, factors such as increasing internet penetration, young demography, digital initiatives and local language computing are projected to throw several opportunities and challenges to the law enforcement agencies in countering national security threats.

Opportunities:

- **Increased engagement with citizens:** The social media enables increased engagement with citizens to build secure communities, which share information that may be used to support investigations.

- **Improved intelligence capabilities:** It offers real-time, first-hand information, which can be used for developing “actionable intelligence” regarding possible flash points of disturbances by using tools such as big data analysis etc. and sharing across agencies.

- **Enhanced preparedness:** It may also be used to prevent misuse of social platforms to spread malicious rumours, which may trigger problems for internal security and law and order, and prepare standard operating procedures for times of emergency.

Challenges:

- **Increased number of cyber-crimes:** Criminals are using social media for sale of contraband items, selection of targets and victims, spreading malware, committing cyber frauds, impersonation, hacking etc. For example, recently, Pakistan has been found 'honey trapping' Indian soldiers, scientists etc.

- **Unregulated space for propaganda:** Terrorists and extremists are using social media to propagate their ideology and recruit members. For example, radicalisation done by ISIS and use of tremendous online following by Burhan Wani to strengthen Hizbul Mujahideen in Kashmir Valley.

- **Fast paced spread of misinformation:** Foreign entities are using social media as a weapon in their psychological operations to cause unimaginable disruptions. For e.g. Pakistan’s ISI uploaded fake inflammatory videos, which triggered exodus of people from North-eastern India staying in Bangalore and Pune.

- **Ineffective laws:** The Indian legal framework that includes IT Act, 2000 and National Cyber Security Policy, 2013 is both inadequate and face limitations in present circumstances. For e.g. denial by WhatsApp to help trace the origin of posts which led to lynching of 5 men in Maharashtra.
Democratic rights: It is also difficult for India to strictly regulate the social media because freedom of speech and privacy are fundamental rights.

Steps taken by India:

NETRA (NETworkTRaffic Analysis): This software has been developed by DRDO in 2014 and is being used by IB and R&AW for real-time detection of suspicious “keywords” and “keyphrases” in social media, emails, blogs, tweets, instant messaging services, and in other types of Internet content.

Social Media Labs: They are used to detect suspicious activity, and track mobilisation using social media for protests, and support domestic law enforcement.

Crime and Criminal Tracking Network System (CCTNS): Launched in 2009, one of the stated goals of CCTNS is predictive policing i.e. real time tracking of internet data including social media data, for domestic law enforcement.

The Government of India is planning to bring comprehensive Social media Regulations and a National Cyber Security Strategy by 2020. A National Media Analytics Centre (NMAC) has also been proposed by the National Security Council.
Heartiest Congratulations to our successful students!

7 in Top 10 Selections in CSE 2019

- Jatin Kishore (AIR 2)
- Pratibha Verma (AIR 3)
- Vishakha Yadav (AIR 6)
- Ganesh Kumar Baskar (AIR 7)
- Abhishek Saraf (AIR 8)
- Ravi Jain (AIR 9)
- Sanjita Mohapatra (AIR 10)

9 in Top 10 Selections in CSE 2018

- Kanishak Kataria (AIR 1)
- Akshat Jain (AIR 2)
- Junaid Ahmad (AIR 3)

Heartiest Congratulations to our successful students!