THE HINDU

Date:11-02-21

Disinformation is a cybersecurity threat

Society needs to be protected from infodemics, to prevent the possibility of a breakdown, interruptions and violence

Ashish Jaiman, [Technologist and innovator, is the Director of Technology and Operations for the Customer Security and Trust organisation at Microsoft]

Cybersecurity focuses on protecting and defending computer systems, networks, and our digital lives from disruption. Nefarious actors use attacks to compromise confidentiality, the integrity and the availability of IT systems for their benefit. Disinformation is, similarly, an attack and compromise of our cognitive being. Nation-state actors, ideological believers, violent extremists, and economically motivated enterprises manipulate the information ecosystem to create social discord, increase polarisation, and in some cases, influence the outcome of an election.

There is a lot of similarity in the strategies, tactics and actions between cybersecurity and disinformation attacks. Cyberattacks are aimed at computer infrastructure while disinformation exploits our inherent cognitive biases and logical fallacies. Cybersecurity attacks are executed using malware, viruses, trojans, botnets, and social engineering. Disinformation attacks use manipulated, miscontextualised, misappropriated information, deep fakes, and cheap fakes. Nefarious actors use both attacks in concert to create more havoc.

Historically, the industry has treated these attacks independently, deployed different countermeasures, and even have separate teams working in silos to protect and defend against these attacks. The lack of coordination between teams leaves a huge gap that is exploited by malicious actors.

Cognitive hacking

Cognitive hacking is a threat from disinformation and computational propaganda. This attack exploits psychological vulnerabilities, perpetuates biases, and eventually compromises logical and critical

thinking, giving rise to cognitive dissonance. A cognitive hacking attack attempts to change the target audience's thoughts and actions, galvanise societies and disrupt harmony using disinformation. It exploits cognitive biases and shapes people by perpetuating their prejudices. The goal is to manipulate the way people perceive reality. The storming of the U.S. Capitol by right-wing groups on January 6, 2021, is a prime example of the effects of cognitive hacking.

The implications of cognitive hacking are more devastating than cyberattacks on critical infrastructure. The damage wrought by disinformation is challenging to repair. Revolutions throughout history have used cognitive hacking techniques to a significant effect to overthrow governments and change society. It is a key tactic to achieve major goals with limited means.

For example, QAnon spread false information claiming that the U.S. 2020 presidential election was fraudulent, and conspiracy theorists (in the United Kingdom, the Netherlands, Ireland, Cyprus and Belgium) burned down 5G towers because they believed it caused the novel coronavirus pandemic. COVID-19 disinformation campaigns have prevented people from wearing masks, using potentially dangerous alternative cures, and not getting vaccinated, making it even more challenging to contain the virus.

Spreading disinformation

Distributed Denial-of-Service (DDoS) is a well-coordinated cybersecurity attack achieved by flooding IT networks with superfluous requests to connect and overload the system to prevent legitimate requests being fulfilled. Similarly, a well-coordinated disinformation campaign fills broadcast and social channels with so much false information and noise, thus taking out the system's oxygen and drowning the truth.

The advertisement-centric business modes and attention economy incentivise malicious actors to run a sophisticated disinformation campaign and fill the information channels with noise to drown the truth with unprecedented speed and scale.

Disinformation is used for social engineering threats on a mass scale. Like phishing attacks, to compromise IT systems for data extraction, disinformation campaigns play on emotions, giving cybercriminals another feasible method for scams.

A report (https://bit.ly/3q9Tg3B) released by Neustar International Security Council (NISC) found 48% of cybersecurity professionals regard disinformation as threats, and of the remainder, 49% say that threat is very significant; 91% of the cybersecurity professionals surveyed called for stricter measures on the Internet.

Deep fakes add a whole new level of danger to disinformation campaigns. A few quality and highly targeted disinformation campaigns using deepfakes could widen the divides between peoples in democracies even more and cause unimaginable levels of chaos, with increased levels of violence, damage to property and lives.

Lessons from cybersecurity

Cybersecurity experts have successfully understood and managed the threats posed by viruses, malware, and hackers. IT and Internet systems builders did not think of security till the first set of malicious actors began exploiting security vulnerabilities. The industry learned quickly and invested profoundly in

security best practices, making cybersecurity a first design principle. It developed rigorous security frameworks, guidelines, standards, and best practices such as defense-in-depth, threat modelling, secure development lifecycle, and red-team-blue-team (self-attack to find vulnerabilities to fix them) to build cybersecurity resilience. ISACs (Information sharing and analysis centers) and global knowledge base of security bugs, vulnerabilities, threats, adversarial tactics, and techniques are published to improve the security posture of IT systems.

We can learn from decades of experience in the cybersecurity domain to defend, protect and respond, and find effective and practical solutions to counter and intervene in computational propaganda and infodemics. We can develop disinformation defence systems by studying strategy and tactics to understand the identities of malicious actors, their activities, and behaviours from the cybersecurity domain to mitigate disinformation threats. By treating disinformation as a cybersecurity threat we can find effective countermeasures to cognitive hacking.

Defense-in-depth is an information assurance strategy that provides multiple, redundant defensive measures if a security control fails. For example, security firewalls are the first line of defence to fend off threats from external systems. Antivirus systems defend against attacks that got through the firewalls. Regular patching helps eliminate any vulnerabilities from the systems. Smart identity protections and education are essential so that users do not fall victim to social engineering attempts.

We need a defense-in-depth strategy for disinformation. The defense-in-depth model identifies disinformation actors and removes them. Authenticity and provenance solutions can intervene before disinformation gets posted. If the disinformation still gets by, detection solutions using humans and artificial intelligence, internal and external fact-checking can label or remove the content.

Today, the response to disinformation is in silos of each platform with little or no coordination. There is no consistent taxonomy, definitions, policy, norms, and response for disinformation campaigns and actors. This inconsistency enables perpetrators to push the boundaries and move around on platforms to achieve their nefarious goals. A mechanism like ISACs to share the identity, content, context, actions, and behaviours of actors and disinformation across platforms is needed. Information sharing will help disinformation countermeasures to scale better and respond quickly.

Education is key

A critical component of cybersecurity is education. Technology industry, civil society and the government should coordinate to make users aware of cyber threat vectors such as phishing, viruses, and malware. The industry with public-private partnerships must also invest in media literacy efforts to reach out to discerning public. Intervention with media education can make a big difference in understanding context, motivations, and challenging disinformation to reduce damage. The freedom of speech and the freedom of expression are protected rights in most democracies. Balancing the rights of speech with the dangers of disinformation is a challenge for policymakers and regulators. There are laws and regulations for cybersecurity criminals. More than 1,000 entities have signed the Paris Call for Trust and Security in Cyberspace, for stability and security in the information space. Similarly, 52 countries and international bodies have signed the Christchurch Call to Action to eliminate terrorist and violent extremist content online.

The disinformation infodemic requires a concerted and coordinated effort by governments, businesses, non-governmental organisations, and other entities to create standards and implement defences. Taking

advantage of the frameworks, norms, and tactics that we have already created for cybersecurity is the optimum way to meet this threat. We must protect our society against these threats or face the real possibility of societal breakdown, business interruption, and violence in the streets.

Date:11-02-21

Media as target

There must be no room for suspicion that agencies are being used for curbing dissent

Editorial

Ordinarily, searches and seizures are the legitimate starting point of an investigation, done on the basis of prior information. But the ED's raids in the office of independent digital news platform NewsClick, and in the residence of its promoter and editor-in-chief, have invited justified condemnation from organisations representing the media. There is every likelihood that this operation is linked to the platform's in-depth coverage of ongoing protests as well as the various struggles of the people and the grassroot organisations that represent them. Ostensibly arising from an FIR registered by the Delhi police some months ago, the ED is said to be investigating alleged money-laundering to the tune of rs30 crore. Not much is known about the nature of the police case, but the agency is empowered by the Prevention of Money-Laundering Act to investigate if the proceeds of crime related to a 'predicate offence' have been laundered. Whether such a primary offence has been established or not, and if so, whether NewsClick is in any way linked to it, is unclear. However, in the light of the manner in which the central agency is wont to enter the scene to investigate both real and imaginary allegations against anyone vocally critical of the government, it is difficult to brush aside the suspicion that the website is being targeted for its coverage of the farmers' agitation as well as last year's country-wide protests against the Citizenship (Amendment) Act.

The present regime's record is quite dismal when it comes to the obvious use of central agencies such as the CBI, ED, IT and even the NIA, to rein in dissenting voices. It is unfortunate that specialised agencies are allowing themselves to be used as force multipliers in political battles against sections of the Opposition. Amidst claims that there are varying kinds of conspiracies against the government and India, it is no surprise that relentless journalistic focus on protests, which are basically steps taken in pursuit of redress for public grievances, is inviting repressive action. Laws that are serious in nature and ought not to be invoked lightly are being used with abandon against those seen to have invited the establishment's wrath. This may explain the frequency with which the offence of sedition is being invoked for speeches and writings, while allegations of anti-national activity peddled by those groomed to build such narratives lead to action under the Unlawful Activities (Prevention) Act. In other instances, cases of promoting social enmity or outraging religious sentiments are also slapped selectively to 'discipline' comedians and script-writers. The Supreme Court's intervention has protected prominent journalists from arrest for defamation for tweets that turned out to be incorrect. It no more behoves a responsible and responsive government to dismiss criticism of its treatment of dissenters, including journalists who do not agree with it, as motivated or inspired by foreign elements.

Date:11-02-21

Denying women the right over their bodies

Neither the state nor doctors have any right to deny a woman a safe abortion

Thamizhachi Thangapandian, [T. Sumathy aka Thamizhachi Thangapandian is an academic, Tamil poet, an MP (South Chennai constituency), and member of the Standing Committee (Information and Technology)]

Recently, Argentina's Congress legalised abortions up to the 14th week of pregnancy. The Indian Parliament too will consider an amendment to our abortion laws this Budget Session but unlike the Argentina law which is touted as being historic, the Medical Termination of Pregnancy (Amendment) Bill, 2020 (MTP Bill), will not translate into greater autonomy for women over their own bodies.

History of the law

The MTP Act of 1971 was framed in the context of reducing the maternal mortality ratio due to unsafe abortions. It allows an unwanted pregnancy to be terminated up to 20 weeks of pregnancy and requires a second doctor's approval if the pregnancy is beyond 12 weeks. Further, it only allows termination when there is a grave risk to the physical or mental health of the woman or if the pregnancy results from a sex crime such as rape or intercourse with a mentally challenged woman.

Therefore, the law is framed not to respect a woman's right over her own body but makes it easier for the state to stake its control over her body through legal and medical debates. Suppose a woman has had voluntary sex and she decides, for personal reasons, to end her pregnancy. If she is 24 weeks pregnant, then this would be a criminal offence. So, she moves the court under the condition that the pregnancy was affecting her mental health. However, here the court can refuse her despite the woman's choice to end it.

In one such case, a State government had argued that there were no grounds for an abortion since the pregnancy was the outcome of a voluntary act and she was "very much aware of the consequence" and the court agreed.

In such circumstances, women usually resort to unsafe methods of abortion. Unsafe abortions are the third largest cause of maternal deaths in India.

The amendment too continues this legacy of hetero-patriarchal population control, which does not give women control over their own bodies. The proposed amendment still requires one doctor to sign off on

termination of pregnancies up to 20 weeks old, and two doctors for pregnancies between 20 and 24 weeks old. Thus, it is not based on any request or isn't at the pregnant person's will but on a doctor's opinion.

Personal beliefs

The Bill also mandates the government to set up a medical board in every State and UT. Medical boards can rely on the facts of the case but personal beliefs could impact the medical board's opinion, which is one of the biggest challenges in having a third-party opinion on a decision which is very personal. For instance, the Madhya Pradesh High Court denied permission for terminating a 26-week-old pregnancy to a 13-year-old rape survivor with the psychiatrist on the medical board arguing against the mental and emotional trauma that the survivor would go through. The psychiatrist stated that while the survivor was "feeling anxiety at times", she was "not suffering from delusion and hallucination".

While the current Bill provides that safe abortions can be performed at any stage of the pregnancy in case of foetal "abnormalities," it fails to consider any other reason such as personal choice, a sudden change in circumstances due to separation from or death of a partner, and domestic violence.

Last, the proposed amendment uses the word "women" throughout, denying access to safe abortion to transgender, intersex and gender diverse persons.

Abortion rights are central to a woman's autonomy to determine her life's course. Neither the state nor doctors have any right to deny a woman a safe abortion. Doing so means that women are not being treated properly as adults who are responsible for their own choices.

दैनिक भास्कर

Date:11-02-21

कृषि कानून सिर्फ इंटरनेट मीम बनाने के लायक नहीं हैं

चेतन भगत, (अंग्रेजी के उपन्यासकार)

मैं आज बहुत नाराज हूं। हालांकि, इससे पहले कि मैं अपनी नाराजगी जाहिर करूं, यह रहा कुछ सकारात्मक। मैं आपसे कुछ साधारण भारतीय कृषि उत्पादों को वैश्विक ब्रांड बनाने की संभावनाओं के बारे में बात करना चाहता हूं। ये हैं वे 10 भारतीय कृषि उत्पाद जिनमें अरबों डॉलर के ब्रांड बनने की क्षमता है।

1. **आम:** भारतीय आम बेहद स्वादिष्ट होते हैं, उनकी कई किस्में आती हैं। अभी केवल अल्फांसो ही छोटा-मोटा ब्रांड बना है और बाकी में भी क्षमता है।

2. **गाजर:** भारतीय गाजरें खूबसूरत लाल रंग की, कुरकुरी और स्वादिष्ट होती हैं। विदेश में गाजर नारंगी होती हैं और प्लास्टिक जैसी बेस्वाद। भारतीय गाजरें राज कर सकती हैं।

3. **मसाले:** जीरा, लौंग, इलायची... भारतीय मसालों की लंबी फेहरिस्त है। भारत का मसालों से संबंध अच्छे से स्थापित है, पर हम इसका पूरा दोहन नहीं कर पाए।

4. **डेयरी:** हम दुनिया का सर्वश्रेष्ठ चीज, बटर, दही, पनीर और घी बना सकते हैं। अगर ग्रीक योगर्ट मल्टी-बिलियन ब्रांड बन सकता है, तो भारतीय योगर्ट क्यों नहीं?

5. **जामुन:** जामुन जैसे फलों को विदेश में कम जानते हैं, लेकिन उसके कई स्वास्थ्य लाभ हैं। दुनिया का परिचय भारत के असाधारण फलों से कराकर ब्रांड बना सकते हैं।

6. **राजगिरा, अमरनाथ और अन्य हाई-प्रोटीन अनाज:** क्विनोआ को लेकर दुनिया में बहुत उत्साह है। हमारे पास क्विनोआ के बेहतर विकल्प हैं।

7. **चावल:** भारतीय बासमती लंबा, सुंदर, खुशबूदार है। दुनिया में कोई चावल इसके आसपास भी नहीं है।

8. **मिर्च:** भारत के उत्तर-पूर्व में कुछ अनूठे स्वाद वाली मिर्च हैं। हमने उन्हें अभी भारत में ही बेचना शुरू नहीं किया। हम भारतीय मिर्च को भी वैश्विक बना सकते हैं।

9. **सेब:** भारतीय कश्मीरी सेबों के बारे में जानते हैं। दुनिया अभी नहीं जानती।

10. **संतरे:** नागपुरी संतरे स्वाद में स्पेनिश से बेहतर हैं और उन्हें छीलना आसान है।

यह फेहरिस्त लंबी हो सकती है। बात यह है कि भारतीय खेतों में कई अरबों के व्यापार खड़े होने को तैयार हैं। अगर ये बनते हैं तो कौन अमीर होगा? जी हां, बेशक बिजनेस के मालिक लेकिन किसान भी अमीर होंगे। तो ये बिजनेस कैसे बनेंगे? ये प्राइवेट सेक्टर की भागीदारी के बिना नहीं बनेंगे। और इस भागीदारी के लिए हमें लंबित कृषि क्षेत्र सुधारों की जरूरत है।

अब, जब ये सामने हैं तो कई पढ़े-लिखे, वैश्विक रूप से जागरूक लोग उन्हें आगे नहीं बढ़ने दे रहे। यही मेरी नाराजगी का कारण है। सोशल मीडिया पर कृषि कानूनों के खिलाफ शोर ने मुझे बहुत खफा किया। लोग अधपकी समझ के साथ उन कानूनों पर बोल रहे हैं, जिन्हें वे खुद पूरी तरह नहीं समझते।

वैश्विक पॉप स्टार और अन्य इंफ्ल्यूएंसर (सोशल मीडिया पर प्रभावशाली) भारतीय कृषि कानूनों के खिलाफ पोस्ट कर रहे हैं। ऐसे लगभग सभी लोगों में एक बात समान है- इन सभी ने अपने सोशल मीडिया ब्रांड सोशल जस्टिस वॉरियर (सामाजिक न्याय योद्धा) बनकर स्थापित किए हैं।

इस रणनीति में कुछ गलत नहीं है। इससे अच्छी मार्केटिंग होती है और यह ओरिजिन क्रिएटिव कंटेंट बनाने से तो आसान है। बस इन इंफ्ल्यूएंसर्स को अपनी SJW छवि बनाए रखने के लिए सबूत देने पड़ते हैं, ताकि प्रोफाइल पर एंगेजमेंट रहे।

एंगेजमेंट के लिए ये तस्वीरें/वीडियो इस्तेमाल करते हैं। पुलिस वालों से पिटते बूढ़े किसान की तस्वीर अच्छा काम करती है। ठंड में आग तापती बूढ़ी औरत की तस्वीर, शानदार कंटेंट है। हालांकि, कृषि कानूनों पर वास्तविक दस्तावेज या सकारात्मक-नकारात्मक असरों के विश्लेषण की बात की जाए तो इन्हें उबासी आती है। ऐसे पोस्ट करना या पढ़ना उन्हें बोरियत भरा लगता है।

सच्चे बदलाव के पीछे बहुत सारा बोरियत भरा काम होता है। जी हां, कानूनों को बनाना और लागू करना मीम के लायक, उत्साहजनक या भावुक नहीं है। यह बोरियत भरा है। हालांकि, अंतत: यही असरकारी हैं। कानूनों को इसलिए नापसंद करना कि वे मोदी सरकार ने बनाए हैं या सिर्फ किसी तस्वीर/वीडियो से भावुक हो जाना सही नहीं है।

कृषि कानूनों का पारित होना ऊपर दिए गए मल्टी-डॉलर भारतीय कृषि ब्रांड्स के बनने की गारंटी नहीं है। लेकिन, मैं यह गारंटी देता हूं कि कृषि सुधार कानून पारित नहीं हुए तो ये ब्रांड कभी नहीं बनेंगे। इसलिए विरोध करते समय सावधान रहें। क्या आपको पता है क्या चल रहा है? क्या आप जानते हैं कि किसान कैसे अमीर होंगे? बेशक, निजी क्षेत्र का शोषण एक मुद्दा है, जिसे उठाया जाएगा।

समय के साथ किसानों की निजी फर्म वाली प्रतिष्ठा हो जाएगी। लेकिन भगवान के लिए, भारतीय किसानों को अमीर बनाने की सिर्फ बातें न करें। उन्हें अमीर बनाने के लिए काम करें। और उनकी बात सुनें जो 'वर्क' (काम) करते हैं, न कि सिर्फ 'ट्वर्क' (सोशल मीडिया पर प्रचलित डांस का प्रकार)।

दैनिक जागरण

Date:11-02-21

चीन के चंगुल में न फंसने पाए म्यांमार

ब्रह्मा चेलानी, (लेखक सामरिक मामलों के विश्लेषक हैं)

बीते दिनों म्यांमार में हुए सैन्य तख्तापलट के साथ ही कई सवाल उठने लगे हैं। इनमें एक प्रश्न यह है कि क्या भारत के इस अहम पड़ोसी देश पर पश्चिमी देश प्रतिबंध लगाएंगे और वह फिर से अंतरराष्ट्रीय स्तर पर अलग-थलग पड़ जाएगा और वहां वैसे हालात बन जाएंगे जैसे लोकतंत्र की शुरुआत से पहले बने हुए थे? 2010 में भारत यात्रा के दौरान तत्कालीन अमेरिकी राष्ट्रपति बराक ओबामा ने म्यांमार के साथ सक्रिय संवाद वाली भारतीय नीति की आलोचना की थी। हालांकि कुछ महीनों के भीतर खुद ओबामा ने भी वैसी ही नीति अपनाई। फिर 2012 में उनका ऐतिहासिक म्यांमार दौरा हुआ। अब म्यांमार पर प्रतिबंधों का साया फिर से मंडरा रहा है तो क्या इतिहास खुद को दोहराएगा?

भारत की 1,643 किमी लंबी सीमा म्यांमार से लगती है। दोनों देशों के बीच बंगाल की खाड़ी में 725 किमी लंबी तट रेखा भी है। नई दिल्ली म्यांमार को दक्षिणपूर्व एशिया में अपने द्वार के रूप में भी देखती है। भारत अपनी 'एक्ट ईस्ट नीति' के माध्यम से व्यापक आर्थिक एकीकरण में भी लगा है। म्यांमार और भारत के समक्ष कई साझा खतरे भी हैं। इनमें से एक ताकतवर होते बिगड़ैल चीन से भी है।

म्यांमार प्राकृतिक संसाधनों से समृद्ध है। हालांकि आजादी के बाद से ही यहां सेना को छोड़कर कोई अन्य संस्थान फला-फूला नहीं। यहां विभिन्न मतों और नस्ल वाले लोग रहते हैं। उत्तरी एवं पूर्वोत्तर के इलाकों में नस्लीय अलगाववाद की समस्या भी है। हालांकि सेना ने एक दशक पहले देश में चरणबद्ध रूप से लोकतांत्रिक प्रक्रिया को शुरू किया, फिर भी पश्चिमी देशों ने सेना के साथ रिश्ते सहज करने की दिशा में कदम नहीं बढ़ाए। उन्होंने सिर्फ आंग सान सू की पर ही पूरा दांव लगाया। हालांकि वर्ष 2017 में रोहिंग्या के मसले पर सू की के रवैये से भी उन्हें निराशा ही हाथ लगी।

रोहिंग्या को म्यांमार से बड़ी तादाद में बेदखल करने के वाकये ने 1960 के दशक में म्यांमार से पलायन करने वाले पांच लाख से अधिक भारतीय मूल के लोगों की यादें ताजा करा दी थीं। उस समय म्यांमार सैन्य तानाशाह नेविन की मुट्ठी में था, जिसने 1962 में सत्ता हासिल की। इसके बाद 26 वर्षों तक म्यांमार पूरी दुनिया से कटा रहा। म्यांमार के बर्मीकरण की प्रक्रिया में भारतीयों को वहां से भगाया जा रहा था। नेविन ने भारतीयों को उत्पीड़न का शिकार बनाया। उसने निजी उद्योगों का राष्ट्रीयकरण करना शुरू कर दिया। इसका मकसद संपन्न भारतीयों को विपन्न बनाकर वहां से भागने पर विवश करना था। इसके चलते भारत सरकार को भारतीय मूल के लोगों को वहां से लाने के लिए विमान और नौकाएं भेजनी पड़ीं।

1988 तक आते-आते नेविन की विदाई हो गई। तब तक म्यांमार की गिनती दुनिया के दस सबसे गरीब मुल्कों में होने लगी। अनैतिक इतिहास के बावजूद भारत ने अपने हितों को देखते हुए म्यांमार के सैन्य नेतृत्व के साथ सहयोग बढ़ाया। चार महीने पहले ही भारत ने एक किलो क्लास पनडुब्बी की मरम्मत कराकर उसे म्यांमार को उपहारस्वरूप भेंट किया। यह म्यांमार की पहली पनडुब्बी है। भारत ने पिछले महीने ही 15 लाख कोरोना वैक्सीन मुफ्त में म्यांमार को उपलब्ध कराइ हैं। गत वर्ष अक्टूबर में भारतीय सेना प्रमुख और विदेश सचिव ने म्यांमार का दौरा किया था। यह एक महत्वपूर्ण घटनाक्रम था। ध्यान रहे कि चीन उत्तरी म्यांमार में विद्रोही समूहों को मदद पहुंचाता है। ये विद्रोही भारत के खिलाफ भी मोर्चा खोल सकते हैं। असल में वे भारत-म्यांमार सीमा के दोनों ओर सक्रिय हैं। इसे देखते हुए भारत को म्यांमार की सेना के सहयोग की दरकार है।

बीते दिनों हुए सैन्य तख्तापलट ने म्यांमार को लेकर अमेरिकी नीति की एक बड़ी खामी को उजागर कर दिया। वह सैन्य नेतृत्व के साथ कोई कड़ी नहीं जोड़ सका। वास्तव में अमेरिका नवंबर 2019 तक म्यांमार के शीर्ष सैन्य नेतृत्व पर शिकंजा कसे रहा। रोंहग्या मुसलमानों के दमन को नस्लीय सफाया करार देकर उसने दिसंबर 2017 से जनरलों पर वीजा प्रतिबंध लगाए रखने के साथ ही देश पर आर्थिक प्रतिबंध भी जारी रखे। अमेरिका इस सच्चाई को समझने में नाकाम रहा कि म्यांमार में लोकतंत्र को कायम रखने में सेना का सहयोग आवश्यक होगा, अन्यथा वहां सैन्य शासन वापस लौट आएगा। लोकतंत्र को सैन्य नेतृत्व के निरंतर समर्थन के एवज में उसे प्रोत्साहन देने के बजाय अमेरिका उलट व्यवहार ही करता रहा।

म्यांमार को लेकर गलत अमेरिकी आकलन ने नए सैन्य शासन के साथ वाशिंगटन के लिए बहुत कम गुंजाइश छोड़ी है। अमेरिका अगर फिर से 2012 से पहले वाले प्रतिबंधों के उस दौर में वापस लौटता है जब 25 वर्षों की पश्चिमी सख्ती के कारण म्यांमार को बड़ी हिचक के साथ चीन की गोद में जाकर बैठना पड़ा था तो यह अमेरिका का सबसे खराब दांव होगा। ऐसी कोई भी नीति म्यांमार को लेकर अमेरिका की नाकामी को और उलझाएगी। अमेरिका के नेतृत्व में म्यांमार को अलग-थलग करने की कोशिश चीनी तानाशाह शी चिर्नफग को उस देश में आक्रामक रूप से अपने हितों को पोषित करने का अवसर प्रदान करेगी।

म्यांमार की अति-राष्ट्रवादी सेना चीन पर भरोसा नहीं करती। उसका मानना है कि म्यांमार की सेना और सरकार को साधने के लिए ही चीन वहां अलगाववाद को मदद करता है। म्यांमार के जनरलों को असल में चीन के साथ सू की की बढ़ती नजदीकी भी खटक रही थी। यह नजदीकी तब दिखी भी जब 13 महीने पहले शी ने म्यांमार दौरे के दौरान 33 द्विपक्षीय संबंधों पर हस्ताक्षर किए। यह दो दशकों में किसी चीनी नेता का पहला म्यांमार दौरा था। जनरलों ने चीन पर म्यांमार की निर्भरता घटाने के लिए ही लोकतांत्रिक प्रक्रिया शुरू की थी, ताकि वे लोकतांत्रिक देशों के साथ संबंध बढ़ाकर अपनी विदेश नीति को संतुलन दे सकें। ऐसे में यह उनके लिए अंतिम विकल्प होगा कि उनका देश फिर से चीन के साये में चला जाए।

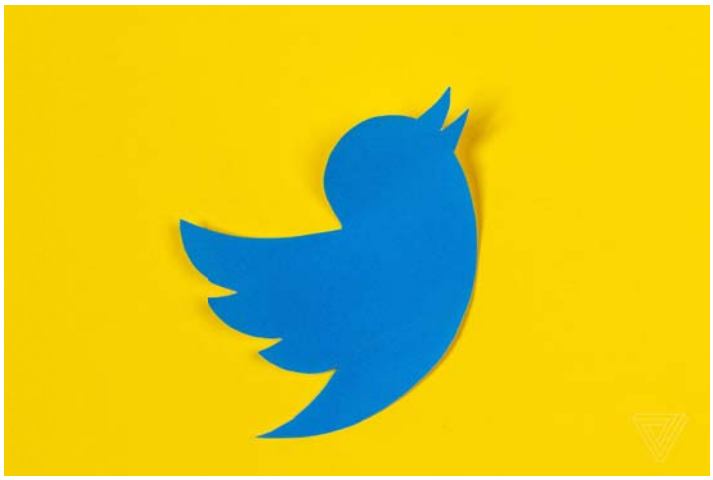
ऐसे परिदृश्य में भारत को अमेरिका को इसके लिए समझाना चाहिए कि म्यांमार को लेकर प्रतिबंधों के बजाय प्रोत्साहन आधारित दूरदर्शी एवं व्यावहारिक रणनीति अपनाने की दरकार है। अमेरिकियों को भारत और जापान जैसे अपने उन मित्र देशों के साथ अवश्य परामर्श करना चाहिए, जिन्होंने म्यांमार में भारी निवेश किया है और उसके सैन्य नेतृत्व से बढ़िया रिश्ते बनाए हैं। भारत और जापान की नीतियों की धुरी रणनीतिक रूप से इस अहम देश में चीनी प्रभाव की काट करने पर टिकी हुई है।

Live हिन्दुस्तान .com

Date:11-02-21

मनमानी के खिलाफ

संपादकीय



भारत सरकार के निर्देश के बावजूद किसी सोशल मीडिया प्लेटफॉर्म की मनमानी या बहानेबाजी चिंता और विचार की बात है। सरकार और ट्विटर के बीच फिर एक बार ठन गई है। 26 जनवरी को लाल किले और दिल्ली में हिंसा के खिलाफ कदम उठाते हुए भारत सरकार ने सैकड़ों ट्विटर हैंडल पर रोक लगाने का निर्देश दिया था, पर ट्विटर ने निर्देश की पूरी पालना से इनकार कर दिया है। ट्विटर के अनुसार, ये विवादित ट्विटर हैंडल भारत में नहीं, पर दुनिया के दूसरे देशों में यथावत देखे जाएंगे। सरकार चाहती थी कि जिन ट्विटर हैंडल का उपयोग हिंसा भड़काने के लिए किया गया है, उन्हें पूरी तरह से प्रतिबंधित किया जाए। ट्विटर ने भारत सरकार के कानून का ही हवाला देते हुए ऐसे प्रतिबंध लगाने से मना कर दिया है। इतना ही नहीं, उसने अपने ब्लॉग पर भारत सरकार को अभिव्यक्ति की आजादी का पाठ भी पढ़ा दिया है। ट्विटर की यह मनमानी किसी अन्य ताकतवर देश में शायद ही संभव है। उसके अधिकारियों की सरकार से वार्ता होनी थी, पर उसके पहले ही अपने विचार पेश करके उसने आग में घी डालने का काम किया है।

भारत सरकार ने ट्विटर की सफाई या बहानेबाजी पर उचित ही नाराजगी का इजहार किया है। सवाल यह है कि ट्विटर ज्यादा सशक्त है या भारत सरकार? क्या ट्विटर सरकार के आदेश-निर्देश से ऊपर है? सरकार आने वाले दिनों में कदम उठा सकती है, जिससे ट्विटर की परेशानी बढेगी। गौर करने की बात है कि भारत सरकार के मंत्री ने 'कू' नामक भारत निर्मित एप पर ट्विटर को शुरुआती जवाब दिया है। अनेक मंत्री और मंत्रालय भी कू के प्लेटफॉर्म पर जाने लगे हैं। मतलब साफ है, ट्विटर से भारत सरकार की निराशा का दौर आगे बढ़ चला है। यह किसी भी सोशल प्लेटफॉर्म की मनमानी रोकने का एक तरीका हो सकता है, पर ट्विटर की भारत में जो पहुंच है, उसे जल्दी सीमित करना आसान नहीं होगा। दूसरी ओर, ट्विटर को बेहतर जवाब के साथ अपना बचाव करना चाहिए। भारत एक बड़ा लोकतंत्र ही नहीं, बड़ा बाजार भी है। यहां सोशल प्लेटफॉर्म चलाने वाली कंपनियों को ज्यादा संवेदनशील रहने की जरूरत है। कहीं ऐसा न हो कि ये कंपनियां भारत सरकार के आदेशों को ही मानने से इनकार करने लगें। जो ट्विटर हैंडल दिल्ली में हिंसा भड़काने में लगे थे, उनके खिलाफ कुछ कार्रवाई की गई, पर कुछ घंटों के बाद कई हैंडल बहाल कर दिए गए। केंद्र सरकार ने ट्विटर से कार्रवाई करने को फिर कहा, बल्कि उसके खिलाफ दंडात्मक उपायों की चेतावनी भी दी। इसके बावजूद अगर ट्विटर के पास कोई ठोस तर्क है, तो उसे सरकार के साथ बैठकर विवाद को सुलझाना चाहिए। लेकिन अपना जवाब

ब्लॉग के जरिए देकर ट्विटर ने विवाद को बढ़ा दिया है। सरकार को भी अपनी गरिमा का ध्यान रखना होगा। ऐसा नहीं होना चाहिए कि कुछेक ट्वीट के आधार पर मीडिया संस्थानों, पत्रकारों, कार्यकर्ताओं और राजनेताओं के खिलाफ कार्रवाई को अंजाम दिया जाए। सोशल मीडिया पर हिंसा भड़काने की किसी भी साजिश को माकूल जवाब मिलना चाहिए, लेकिन प्रतिकूल या आलोचनात्मक टिप्पणियों को बाधित करना भी कतई ठीक नहीं है। सोशल मीडिया प्लेटफॉर्म पर लोकतांत्रिक शालीनता और सहिष्णुता सुनिश्चित रहनी चाहिए।