Disinformation is a cybersecurity threat

Disinformation:

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.

1. Cyberattacks are aimed at computer infrastructure while disinformation exploits our inherent cognitive biases and logical fallacies.
2. Cybersecurity attacks are executed using malware, viruses, trojans, botnets, and social engineering. Disinformation attacks use manipulated, miss contextualised, 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 posed by 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 in January 2021, is a prime example of the effects of cognitive hacking.

Impact 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,

1. QAnon spread false information claiming that the U.S. 2020 presidential election was fraudulent,
2. 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.
3. 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

1. 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.
2. The advertisement-centric business models 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.
3. Disinformation is used for social engineering threats on a mass scale.
4. Deep fakes add a whole new level of danger to disinformation campaigns. A few quality and highly targeted disinformation campaigns using deep fakes 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

1. 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.
2. 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.

3. By treating disinformation as a cybersecurity threat we can find effective countermeasures to cognitive hacking.
4. We need a defence-in-depth strategy for disinformation. The defence-in-depth model identifies disinformation actors and removes them.
5. If the disinformation still gets by, detection solutions using humans and artificial intelligence, internal and external fact-checking can label or remove the content.
6. A mechanism like Information Sharing and Analysis Centers (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

1. The industry with public-private partnerships must also invest in media literacy efforts to reach out to the discerning public. Intervention with media education can make a big difference in understanding context, motivations, and challenging disinformation to reduce damage.
2. The freedom of speech and 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.

Conclusion:

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.

Background:

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.**

Denying women the right over their bodies

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

Context: 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

1. 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.
2. 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.

Problems in the law:

1. 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.
2. 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.
3. 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.
4. In such circumstances, women usually resort to unsafe methods of abortion. Unsafe abortions are the third largest cause of maternal deaths in India.
5. The amendment continues this legacy of hetero-patriarchal population control, which does not give women control over their own bodies.

6. 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.
7. Last, the proposed amendment uses the word "women" throughout, denying access to safe abortion to transgender, intersex and gender diverse persons.

Personal beliefs

1. 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.
2. 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.

Conclusion:

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.

Taking the long view with China

Bottom Line: Both Asian giants can share prosperity and be independent of each other and of the West.

Axes of Indian Geopolitics:

1. **India for a Multipolar world and Multipolar Asia:** Both India and China should remain committed to a multipolar world, they should recognise that a "multipolar Asia" was one of its essential constituents.
2. India has a "special and privileged strategic partnership" with Russia, which provides more than three-quarter of India's military equipment, and a "comprehensive global strategic partnership" with the U.S.

3. India's relationship with the U.S.-led Quadrilateral Security Dialogue (Quad), where the others are military allies, has rightly been cautious. Realism dictates that India does not need to compromise on its strategic autonomy.

Diplomatic challenge: Chinese Dominance

1. The foreign policy challenge for India is really two sides of the China conundrum: defining engagement with its neighbour which is consolidating an expanding Belt and Road Initiative (BRI) while remaining involved with the strategic, security and technological concerns of the U.S. located across the vast Pacific Ocean.
2. In the financial sphere, there is the real possibility of the Chinese renminbi becoming a global reserve currency or e-yuan becoming the currency of digital payments. China is the world's largest trading economy. It could soon become the world's largest economy
3. The BRI countries are using the renminbi in financial transactions with China and can be expected to use it in transactions with each other.
4. China has stitched together an investment agreement with the EU and with most of Asia. China, facing technological sanctions from the U.S., may well put in the hard work to make this happen soon.

Some Policy elements for China: Impossibility of China Containment

1. Some form of the EU's China policy of seeing the emerging superpower as a partner, competitor, and economic rival depending on the policy area in question is going to be the global norm.
2. The EU's reaching out to China despite misgivings of the U.S. means the West has given up on containing the rise of China.
3. This broad perspective is also reflected in India's participation in both the Shanghai Cooperation Organisation, led by Beijing and Moscow and designed to resist the spread of Western interests and in the U.S.-led Quad, with its anti-China stance.
4. Within the United Nations, India's interests have greater congruence with China's interests rather than the U.S.'s and the EU's.

India and West

1. The congruence between India and the U.S. lies in the U.S.'s declared strategic objective of promoting an integrated economic development model in the Indo-Pacific as a credible alternative to the BRI.

2. Instead of an alternate development model, India should move the Quad towards supplementing the infrastructure push of the BRI in line with other strategic concerns in the region.
3. For example, developing their scientific, technological capacity and digital economy, based on India's digital stack and financial resources of other Quad members, will resonate with Asia and Africa.

Conclusion:

As in the historical past, Asia is big enough for both Asian giants to have complementary roles, share prosperity and be independent of each other and of the West.