

①

DATE: \_\_\_/\_\_\_/\_\_\_

# Digital Terrorism and Free Speech: Balancing National Security with Civil Liberties

## Outline

### (1) Introduction

### (2) How digital terrorism leaves national security vulnerable

(i) It has enabled non-state belligerent actors to spur unrest.

(ii) Digital terrorism has redefined warfare in an increasingly tech-savvy world.

(iii) Lone-wolf terror operations have put counter-terrorism institutions on backfoot.

### (3) Against this backdrop, states have enacted legislations to rein in digital terrorism, much to the detriment of civil liberties: Manifestation

(i) European Parliament legislated laws to limit free speech

(ii) China, Iran, Russia and North Korea do not let their citizens access mainstream social media

(iii) Pakistan's Parliament has also introduced laws to keep civil liberties in check.



(4) Thus, there is a need to balance national security with civil liberties:

(i) States around the world should not place sweeping bans on freedom of speech and association.

(ii) Securitization of internet should be subject to constitutional checks and parliamentary oversight.

(iii) States should increase their presence on cyberspace, offering effective counter-narratives to downplay digital terrorism.

(iv) Concerns of digital rights experts must not be brushed aside.

(v) It is advised that democratic values should not be seen as impediment to national security.

(vi) Academics, digital experts, social media sites and states should work in concert to secure democracy and bolster national security.

(5) Conclusion



3

DATE: \_\_\_/\_\_\_/\_\_\_

Donald Trump administration was quick to celebrate the defeat of Islamic state of Iraq and Syria (ISIS) in 2019. President Trump released a video on X (then Twitter) to declare the victory of free-world over sinister designs of terrorist entities. Until did he know that by the time he would secure another victory over his Democrat counterpart, the ISIS will be transformed into a digital caliphate, requiring no territory to advance its ambitions, as witnessed on the eve of New Year when a young man blew himself up in New Orleans. A similar horror also shook Russia in early 2024, manifesting the rise of digital terrorism. However, in addressing this new monster, states have doubled down their efforts to place bar on constitutionally protected freedom of expression and civil liberties in one way or another. European Parliament has legislated laws to protect national security, abandoning the ideals of civil liberties. China and Russia remain overly cautious, while Iran and North Korea have weaponised digital terrorism to gag dissent. Closer to home, Pakistan's Parliament has also introduced a spate of legislations aimed at addressing the question of digital terrorism, sparking debate about the spirit of legislations. At a time when democracies around the world are displaying cracks, the stance of states on civil



liberties risks prompting a wave of authoritarianism. Therefore, there is a need for balancing between the concerns of national security and threats to civil liberties. To this end, states should recognise that placing sweeping restrictions serve no one. The policing and securitization of internet should be subject to constitutional checks. The space for dissenting <sup>voices</sup> must not be abandoned. Effective strategies, in collaboration with activists, experts and academics, could be spelled to find a middle ground, serving national security and democratic values.

Succinctly, this essay argues that digital terrorism has emerged as a threat to national security, prompting states to squeeze democratic norms. The piece advocates for a middle ground, where national security and democracy work in tandem to secure prosperous future.

Undeniably, the emergence of digital terrorism has left national security vulnerable. The tech-savvy non-states actors have used digital sphere to advance their cause. It was manifested on the eve of New Year in New Orleans when a young man recruited on internet by ISIS blew himself up, conveying the message that digital caliphate of



5

DATE: \_\_\_/\_\_\_/\_\_\_

ISIS is alive and kicking. Much similar happened to Russia - a nation ISIS deem a scathing rival. In early 2024, the concert hall of Moscow was bleeded as ISKP cadres came to instill a wave of terror in Russia. The assault resulted in 73 Russians losing their life. Thus, the active participation of non-state violent actors have redefined terrorism.

The concept of warfare has been significantly altered in the aftermath of digital terrorism. The need for directly attacking a nation has diminished, with modern means of warfare, such as digital terrorism, has allowed no avenues for putting rivals on backfoot. India does this meticulously. It involves various mechanism to propagandise against its geopolitical nemesis to erode their national power. EuDisinfo lab discovered how India employed hundreds of thousands AI bots to cultivate the image of Pakistan as a nation supporting terrorism around the world. Similarly, it has



6

DATE: \_\_\_/\_\_\_/\_\_\_

employed similar postures to convey how Chinese are ~~an~~ aggressive in their pursuit of security and global hegemony. With the arrival of hybrid warfare, including digital terrorism, the concept of warfare is, thus, redefined.

The ability of internet to penetrate wide and fast has allowed terrorist entities to recruit lone-wolf capable citizens. They are recruited, prepared and trained on internet to carry out terror attacks. Over the last five years, after the defeat of ISIS in Levant, such operations have found prominence, as terrorists have reaped the dividends of global connectivity. The Council for Relations note that the odds of more lone-wolf attacks, with New Orleans as baseline, are bright. Such operations are hard to detect and deter, given a single individual carries it out. Thus, the rise of lone-wolf demonstrates the threat posed by digital terrorism.



7

DATE: \_\_\_/\_\_\_/\_\_\_

To pushback against the threats to national security emanating from digital terrorism, many states have legislated laws to curb civil liberties.

To begin with, EU has introduced contentious laws to keep the civil liberties in check, sparking debate whether such laws are compatible with the norms of democracy. The 2022 EU Free Speech and Data Protection Act unnerved political scientist the world over. Steven Levitsky in *Journal of Democracy* argues that the enacted law runs contrary to the democratic ideals espoused by the Union. The latter noted the need for such a law was growing, pushing the organisation to put in place mechanism to protect citizen from vulnerabilities of digital terrorism. At the same time, critics argued to EU was abandoning democracy in search for national interest. The discontent over the law manifested the spirit of it, perhaps against civil liberties.



8

DATE \_/ \_/ \_

The nations having a distinct worldview to West, including Russia and China, do not let their citizens to access Westernized mainstream social media platforms. They contend that doing so serves their security interests. However, it is hard not to see the growing democratic deficits in their state policies. Such a proposition is widely used to silence dissenting voices, putting democracies at bay. Iran takes it even further. The securitization of internet in Iran mirrors the policies of an authoritarian regime compromising democratic civil liberties for national security. Thus, the policies of these nations stand as testament to global approach of curbing civil liberties for security.

In Pakistan, such an approach seems permeating the policy discourse, too. The 2024 hard been particularly pronounced in adopting the strategy of giving up on democracy in search for national security interest. Adeel



9

DATE: \_\_\_/\_\_\_/\_\_\_

Malik, Professor of Sociology and Political Science, sees it expansion of de facto powers in Pakistan. The Oxford Professor views a number of legislations, including Peca 2016, as an instrument to cut dissenting voices to size - in an effort to entrench the role of unconstitutional powers. Thus, Pakistan, too, finding it hard to retain democratic liberties following the onslaught of digital terrorism.

After discussing the rise of digital terrorism and state response to it against the ideals of liberal democracy, it is not hard to find gaps between the claims of state to democratic and constitutional right and their susceptibility to dither in the face of headwinds. The discourse below centres on the balancing principle, enabling democracy and national interest to flourish simultaneously.

To this end, it is advised that the states must not introduce sweeping bans - in disregard for civil liberties. Such a policy erode freedom of expression and leaves democracy vulnerable and fragmented.



10

DATE: \_/ \_/ \_

In his seminal work, Nexus, Mr Yuvah Naoh Hazari recalls the threat of sweeping bans as against national security and democracy. He argues that bans serve the interest of non-state actors who get undue attention, which they exploit and find new ideologues. Similarly, such a policy exodes democracy, pitting citizens against states. More nuanced strategies would work. However, sweeping bans are likely to move the needle. Hence; academics do not endorse it.

§ In balancing democratic fundamental rights and interests of national security, the securitization of internet must not be the exclusive mandate of security institutions and executive. There must be a mechanism of checks and balances that citizen's privacy and natural rights are protected. In this regard, Daniel Zabillat, a Political Scientist, argues for the role of parliament and judiciary. He promotes the expansion of judicial authority to keep security



11

DATE: \_\_\_/\_\_\_/\_\_\_

institutions in check. Doing so would serve the interest of national security and democratic civil liberties, offering a balanced approach.

Instead of blanket bans on freedom of expression and right to association, the states are advised to enhance their presence on internet in substantive ways, offering counter-narratives to effectively dilute the appeal of digital terrorist. It requires crafting strategies to identify, locate and serve counter arguments to secure interest of national security. This nuanced strategy will save civil liberties while denouncing digital terrorism. Maleeha Lodhi argues that strategic intervention would balance two competing responses. Türkiye has done it quite brilliantly to pushback Kurdish nationalism without banning the social media sites. Other states should, thus, take a leaf or two from their success.



Similarly, States must not crack down on the democratic voices of digital rights experts in pursuing national security. They must not be viewed as impediment; rather, states should see them important partners and stakeholders capable of aiding states in pushing back digital terrorism. In sharp contrast, however, states are eager to order such dissidents, coercing them to toe the line. Recently, Brazil's X ban invited sweeping opposition. Many experts saw it a draconian measure, prompting the state to instigate range of criminal cases against them on trumped-up charges. Such an approach works to the detriment of national security and democracy. A change in approach along democratic rights is advocated.

In continuation of above argument, as mentioned earlier, states have started seeing realising democratic liberties as rather obstruction to stability and national security - an argument



Mussolini mainstreamed following his ascent to highest democratic and political office of Italy. Today, many states have adopted such an approach. Even the established democracies are having qualms regarding the relationship of open society and democracy. The rise of Fox-Riget is attributed to this. How Democracies Die by Levitsky takes this argument on centre of the debate, noting that democracy serves national security. Thus, adopting a new lens suggesting democratic ideals as partner - not threat, to national security would go a long way in balancing between the concerns of national security and civil liberties.

Finally, there is a great need to engage academics, digital rights experts, technological giants and political and commercial stakeholders in mapping out a nuanced strategy that finds a middle ground between the immediate requirements of national security and health of civil liberties. Maya Tudor, a Political Scientist, argues



in Political Science Review in US that nuanced strategies could only work in the complex society one live. Mr. Haxasi strikes chord with her argument that to achieve a balance, states are ought to take buy-in of all stakeholders to make safety and democracy a lasting reality. Thereby, the argument advocates for engaging multiple stakeholders to craft policies aimed at achieving a significant balance between national security and civil liberties.

In conclusion, it is argued that the rise of digital terrorism is palpable, posing serious threat to national security of nation-states. The latter's response, however, leaves too much to be desired, contributing massively to the rising tide of authoritarianism, even in the established democracies. The basic argument is there is a great deal of literature is available to bridge the gap between concerns of national security and threats to civil liberties. The essay recommends



Strategies to Find a critical balance, enabling democracies to flourish and national security to find firm footing. It promotes the checks and balance of constitutional framework to find that balance, suggesting states to view civil liberties as a partner in addressing the vulnerabilities of national security rather than a threat. The piece also calls for crafting nuanced strategies involving range of stakeholders, scholars and experts in crafting a strategy advancing the cause of national interest and democracy, arguing that a nuanced framework is required to defeat digital terrorism and secure the health of democratic ideals and constitutionally protected civil liberties.