Evolving Landscape of Tech-Terror Nexus and Response Options for Global South

SHARE

Society to Harmonise Aspirations for Responsible Engagement

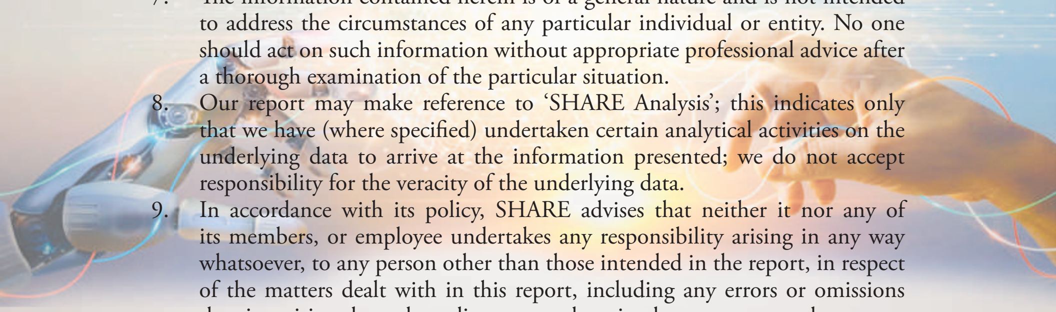
Evolving Landscape of Tech-Terror Nexus and Response Options for Global South

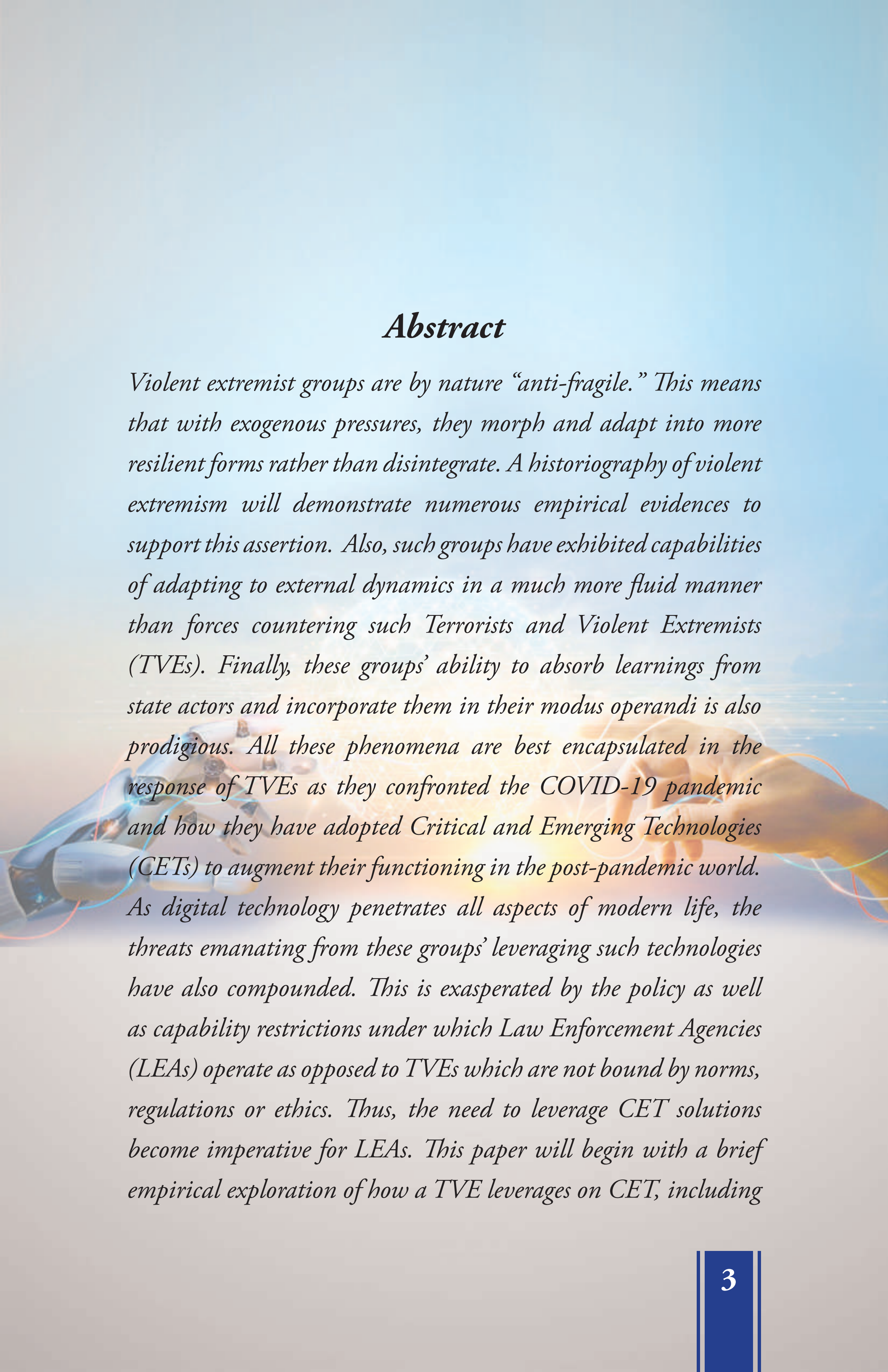
SHARE

Society to Harmonise Aspirations for Responsible Engagement

Disclaimer and Notice to Reader:

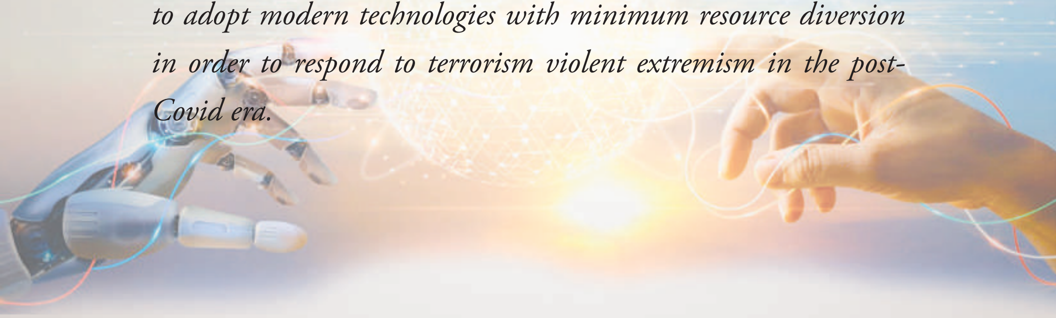
1. This report is for restricted circulation only. It is not to be distributed nor is to be copied, circulated, referred to or quoted in correspondence, or discussed with any other party, in whole or in part, without our prior written consent. Though, Fair Use policies apply.
2. This report sets forth our views based on the completeness and accuracy of the facts stated to SHARE and any assumptions that were included. If any of the facts and assumptions is not complete or accurate, it is imperative that we be informed accordingly, as the inaccuracy or incompleteness thereof could have a material effect on our conclusions.
3. While performing the work, we assumed the genuineness of all signatures and the authenticity of all original documents. We have not independently verified the correctness or authenticity of the same.
4. Comments in our report are not intended, nor should they be interpreted to be legal advice or opinion.
5. While information obtained from the public domain or external sources has not been verified for authenticity, accuracy or completeness, we have obtained information, as far as possible, from sources generally considered to be reliable. We assume no responsibility for such information.
6. Our views are not binding on any person, entity, authority or Court, and hence, no assurance is given that a position contrary to the opinions expressed herein will not be asserted by any person, entity, authority and/or sustained by an appellate authority or a Court of law.
7. The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.
8. Our report may make reference to 'SHARE Analysis'; this indicates only that we have (where specified) undertaken certain analytical activities on the underlying data to arrive at the information presented; we do not accept responsibility for the veracity of the underlying data.
9. In accordance with its policy, SHARE advises that neither it nor any of its members, or employee undertakes any responsibility arising in any way whatsoever, to any person other than those intended in the report, in respect of the matters dealt with in this report, including any errors or omissions therein, arising through negligence or otherwise, howsoever caused.
10. In connection with our report or any part thereof, SHARE does not owe duty of care (whether in contract or in tort or under statute or otherwise) to any person or party to whom the report is circulated to and SHARE shall not be liable to any party who uses or relies on this report. SHARE thus disclaims all responsibility or liability for any costs, damages, losses, liabilities, expenses incurred by such third party arising out of or in connection with the report or any part thereof.
11. By reading our report, the reader of the report shall be deemed to have accepted the terms mentioned hereinabove.





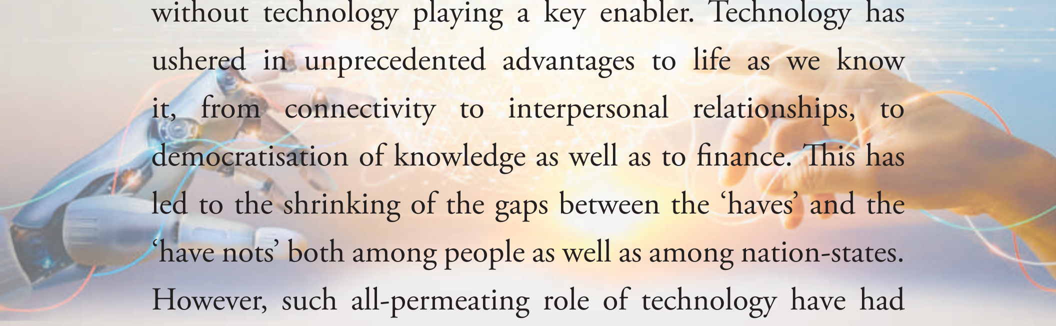
Abstract

Violent extremist groups are by nature "anti-fragile." This means that with exogenous pressures, they morph and adapt into more resilient forms rather than disintegrate. A historiography of violent extremism will demonstrate numerous empirical evidences to support this assertion. Also, such groups have exhibited capabilities of adapting to external dynamics in a much more fluid manner than forces countering such Terrorists and Violent Extremists (TVEs). Finally, these groups' ability to absorb learnings from state actors and incorporate them in their modus operandi is also prodigious. All these phenomena are best encapsulated in the response of TVEs as they confronted the COVID-19 pandemic and how they have adopted Critical and Emerging Technologies (CETs) to augment their functioning in the post-pandemic world. As digital technology penetrates all aspects of modern life, the threats emanating from these groups' leveraging such technologies have also compounded. This is exasperated by the policy as well as capability restrictions under which Law Enforcement Agencies (LEAs) operate as opposed to TVEs which are not bound by norms, regulations or ethics. Thus, the need to leverage CET solutions become imperative for LEAs. This paper will begin with a brief empirical exploration of how a TVE leverages on CET, including *artificial intelligence (AI) in confluence with social media, as well as how it has learnt to adapt to state actions, thus bettering its operational security (OpSec) measures in order to evade the radar of LEAs. The paper then identifies avenues for LEAs to absorb CET in their Counter Violent Extremism (CVE) campaigns effectively and efficiently, while judiciously deploying their finite resources as CVE remains only a part of their larger charter. Here, potential use-cases of CET are highlighted by simulating real world challenges faced by LEAs. The paper is written from the perspective of LEAs, which are generally at the medium or lower strata of the global LEA pyramid in terms of resource availability and capability. Thus, the primary goal of this paper is to provide a use case-based manual for LEAs, especially of the 'Global South,' to adopt modern technologies with minimum resource diversion in order to respond to terrorism violent extremism in the post-Covid era.*



Introduction

From ordering our favourite dish from a fancy new restaurant in town, to booking a holiday with the family, to reconnecting with long lost friends, to scouting professional opportunities, to keeping oneself abreast with the happenings of the day, to seeking out a life partner, there are hardly any aspect of modern life that would seem plausible without technology playing a key enabler. Technology has ushered in unprecedented advantages to life as we know it, from connectivity to interpersonal relationships, to democratisation of knowledge as well as to finance. This has led to the shrinking of the gaps between the 'haves' and the 'have nots' both among people as well as among nation-states. However, such all-permeating role of technology have had impact in creating new insecurities and threats for citizens and their nations alike. From cyber frauds on gullible individuals to cyber-attacks on the power grid of a major city, from



There are hardly any aspect of modern life that would seem plausible without technology playing a key enabler.

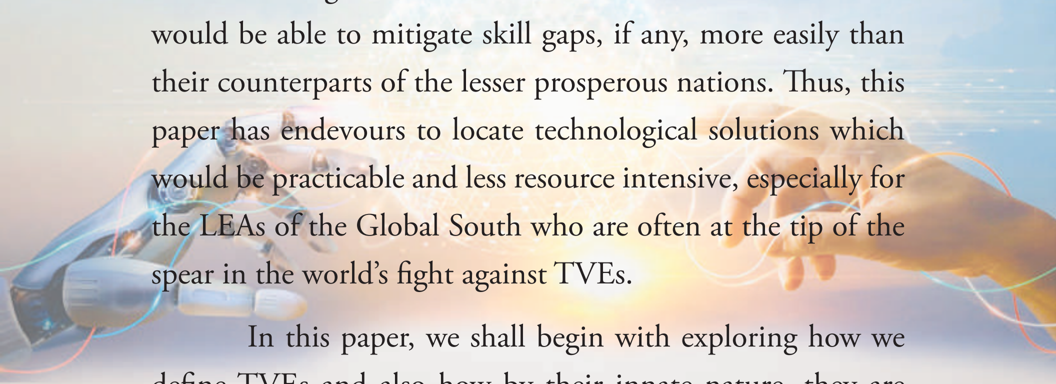
trading narcotics and other contrabands to planning attacks on a certain individuals or groups, the way technology has created new vectors of threats or augmented existing ones, is unprecedented. This is especially true in the AI revolution that we are all witnessing today. While some aspects of CET still remain elusive to the masses, AI and its related sub-streams have become available in the open source quite easily.

These advancements in technology have come as a new found lease of life especially to the TVE actors, who had been bearing the brunt of global action against these groups, curtailing their operational space, their ability to communicate and their avenues to propagate their ideologies in order to recruit fresh crops. With the advancements in technologies like AI, encryptions, cryptocurrencies, unmanned mobility systems, etc., these threat actors have been able to embrace such technological progress and embed them in every aspect of their operation; from propaganda to recruitment, to communication to attack planning and execution as well as finance. In this paper, we will explore various ways and means in which the TVEs have been using the technological leaps of the world to their advancement. The sudden spike in such technological adoption by these bad-faith actors as COVID-19 pandemic hit the world is analysed in some details in this paper as well.

The authors of this paper have found in their research that the ability to counter punch against these TVEs by LEAs

While skill is not a geo-specific marker, it is transient and is influenced by resources. Thus, the LEAs of the more prosperous nations, with greater access to resources in their CVE efforts would be able to mitigate skill gaps, if any, more easily than their counterparts of the lesser prosperous nations.

is not equal among the various agencies of the world. This is primarily because of two factors; skill gap and resource gap. While skill is not a geo-specific marker, it is transient and is influenced by resources. Thus, the LEAs of the more prosperous nations, with greater access to resources in their CVE efforts would be able to mitigate skill gaps, if any, more easily than their counterparts of the lesser prosperous nations. Thus, this paper has endevours to locate technological solutions which would be practicable and less resource intensive, especially for the LEAs of the Global South who are often at the tip of the spear in the world's fight against TVEs.

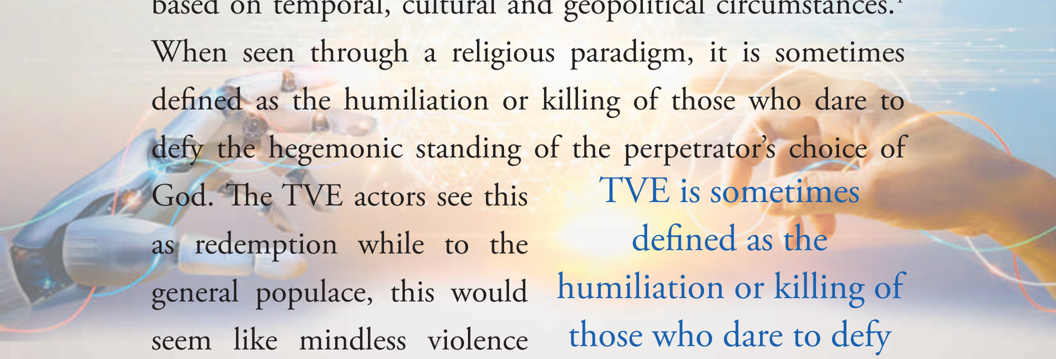


In this paper, we shall begin with exploring how we define TVEs and also how by their innate nature, they are adaptive to exogeneous pressures. We shall cite exhibits from different theaters to make this case. Next, we shall demonstrate how this adaptive ability of the TVE actors were in full display as they responded to the COVID-19 pandemic. Here, we will focus on how they embraced technologies, mostly open source, to further their nefarious designs both in the virtual

The paper also provides the LEAs of the Global South with a usable manual which they may use to adopt some of the tactics, techniques and procedures of the TVEs, innovate upon them by leveraging on their superior resources and in the process, not only defeat the designs of these threat actors but also to edge past some of their counterparts in the Global North, through innovation.

and physical space. Thereafter, we examine how an effective response to such evolving *modus operandi* may be crafted by the LEAs in their mission of countering the TVEs. In doing so, we thrive to draw a distinction between the response and resource capabilities of the LEAs from the 'Global North' and the 'Global South.' Given the palpable disparity in their internal security budgets, those in the Global South will need to forge their own path. Some of those potential approaches are then delt with, in the next section of the paper. Finally, the paper concludes by recognising the fact that the current geopolitical situation will provide further fillip to the TVEs to further their nefarious agenda. However, the paper also provides the LEAs of the Global South with a usable manual which they may use to adopt some of the tactics, techniques and procedures of the TVEs, innovate upon them by leveraging on their superior resources and in the process, not only defeat the designs of these threat actors but also to edge past some of their counterparts in the Global North, through innovation.

Terrorist and Violent Extremist



As we deal with TVE actors, we need to first develop a framework within which to define them. While there is no universally acceptable definition, in this paper, we shall borrow the definition put forward by scholar Randy Borum as this seems to provide a degree of flexibility and evolution. Borum defines TVE as an evolutionary concept that morphs based on temporal, cultural and geopolitical circumstances.[1] When seen through a religious paradigm, it is sometimes defined as the humiliation or killing of those who dare to defy the hegemonic standing of the perpetrator's choice of God. The TVE actors see this as redemption while to the general populace, this would seem like mindless violence and mass slaughter.[2]

TVE is sometimes defined as the humiliation or killing of those who dare to defy the hegemonic standing of the perpetrator's choice of God.

Given this level of conviction

[1] Borum, R. (2011). "Rethinking Radicalization." *Journal of Strategic Security* 4, no. 4: 1-6. http://dx.doi.org/10.5038/1944-0472.4.4.1.

[2] Simon, S. and Benjamin D. (2002). "Age of Sacred Terror." (New York: Random House): 40.

These groups have demonstrated the ability to morph into a loosely connected network which operates fairly independent of a centralised command-and-control structure

of cause among the TVEs, it is only natural that such groups are difficult to obliterate through external force. In fact, these actors absorb such changes in exogenous environment and adapt itself to remain relevant. A case in point would be the famous (or infamous) American War on Terror in Iraq and Afghanistan which, as data would demonstrate have been counter-productive to its proclaimed goals. Data suggests that in the 15 years preceding 9/11 (1986-2001), there were four terror attacks in America killing 10 Americans while in the next 15 years, there were eight attacks killing 88 Americans.[3] Similarly, the number of Islamic terror groups in the world were 13 in the period of 1986-2001. While in 2015, the number had shot up to a staggering 44.[4] Journalist Peter Byrne terms this phenomenon as the 'anti-fragile' nature of these groups.[5] According to Byrne, these groups have

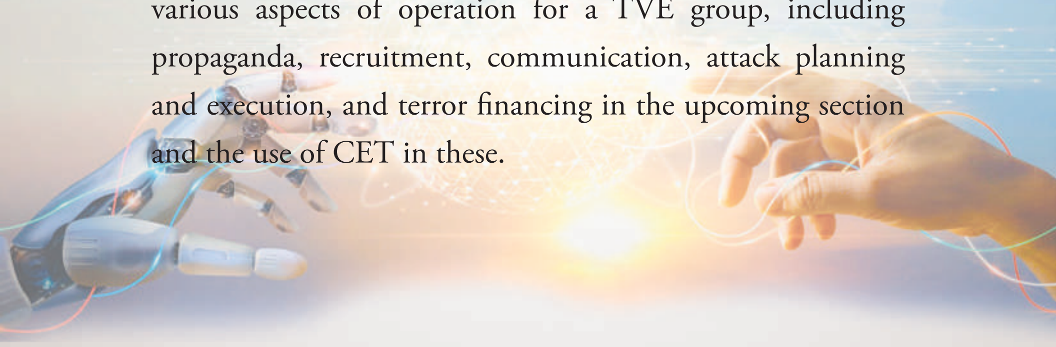
[3] Miller, E. and Jensen, M. (2016). American deaths in terrorist attacks, 1995-2015. In Fact Sheet [Fact Sheet]. *START*. https://www.start.umd.edu/pubs/START_AmericanTerrorismDeaths_FactSheet_Sept2016.pdf.

[4] Thrall, A. T, and Goepner E. (2017). "Step back: lessons for US foreign policy from the failed WoT." *Cato Institute Policy Analysis* 814. https://www.cato.org/policy-analysis/step-back-lessons-us-foreign-policy-failed-war-terror.

[5] Byrne, P. (2017). "Anatomy of terror: What makes normal people become extremists?," *NewScientist*. https://www.newscientist.

demonstrated the ability to morph into a loosely connected network which operates fairly independent of a centralised command-and-control structure at least at an operational level, thus supporting Borum's definition. He further posits that these groups have been the beneficiary of a second order effect of American strategy of surge whereby, the harder they were hit, the easier was their job in recruiting more cadres on their roll.

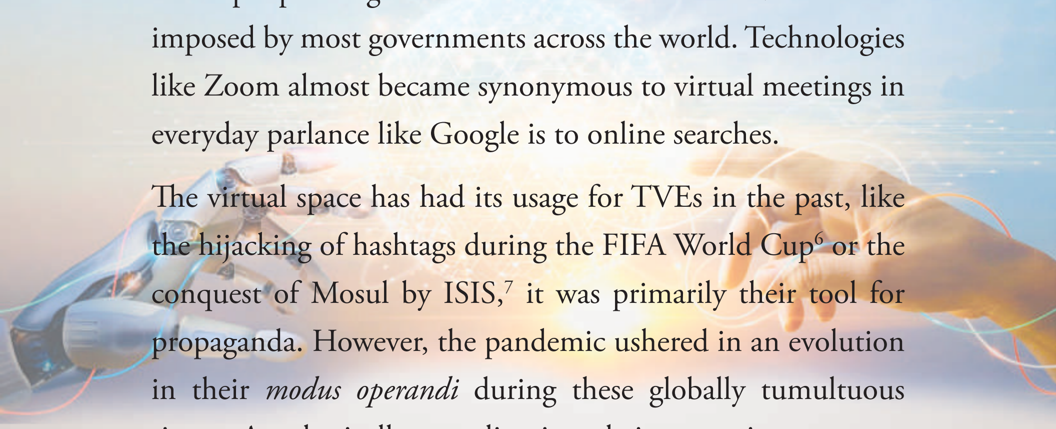
Now that we have established a normative understanding of TVEs in this section, we will explore the TVEs' response to the Covid-19 pandemic and how they embraced CET to further their dastardly design in the next section. We shall explore various aspects of operation for a TVE group, including propaganda, recruitment, communication, attack planning and execution, and terror financing in the upcoming section and the use of CET in these.



com/article/mg23531390-700-anatomy-of-terror-what-makes-normal-people-become-extremists/.

The COVID-19 Impact

In this section, it is argued that one of the most evident exhibitions of this amorphous nature of the TVE groups is how they have responded to the COVID-19 pandemic. The world witnessed a rapid adoption of digital technologies to keep operating at a reasonable rate as lockdowns were imposed by most governments across the world. Technologies like Zoom almost became synonymous to virtual meetings in everyday parlance like Google is to online searches.

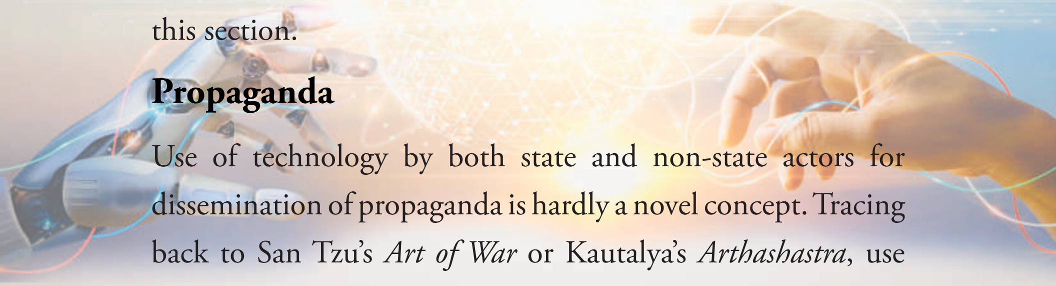


The virtual space has had its usage for TVEs in the past, like the hijacking of hashtags during the FIFA World Cup[6] or the conquest of Mosul by ISIS,[7] it was primarily their tool for propaganda. However, the pandemic ushered in an evolution in their *modus operandi* during these globally tumultuous times. As physically coordinating their operations was no

[6] Milmo, C. (2014). Iraq crisis exclusive: Isis jihadists using World Cup and Premier League hashtags to promote extremist propaganda on Twitter. *The Independent*. https://www.independent.co.uk/news/world/middle-east/iraq-crisis-exclusive-isis-jihadists-using-world-cup-and-premier-league-hashtags-to-promote-extremist-propaganda-on-twitter-9555167.html.

[7] Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. (New York: Eamon Dolan Books): 4-7.

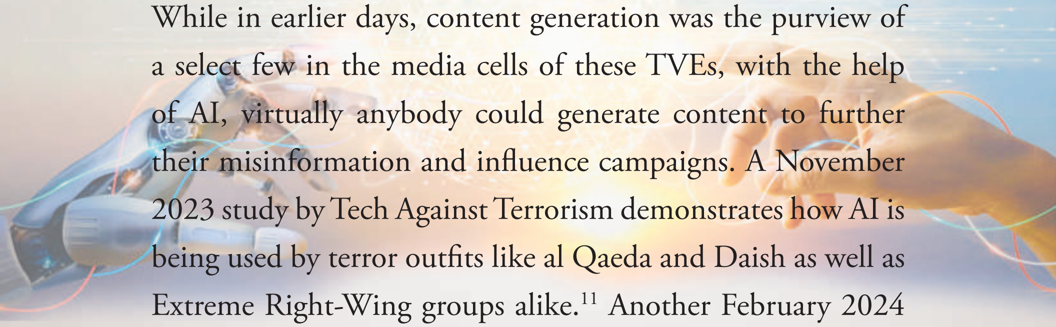
longer possible, they took to the virtual space not just for propaganda and recruitment, it was also the training camps, the operation center as well as the battleground. The choice of weapon for the TVE in this new realm was the ever so ubiquitous technology, Artificial Intelligence (AI) and its multiple sub-streams like Machine Learning (ML), Natural Language Processing (NLP), Neural Networks (NN), etc. In this section, we demonstrate empirical evidences in support of the above assertion. We shall explore how the above technologies have been deployed in multiple spheres of their operation, including propaganda, recruitment, communication, planning, and potentially execution of their dastardly plans as well as terror financing. We will explore each of these operational aspects in the subsequent part of this section.



Propaganda

Use of technology by both state and non-state actors for dissemination of propaganda is hardly a novel concept. Tracing back to San Tzu's *Art of War* or Kautalya's *Arthashastra*, use of propaganda has a long history.[8] The *Ahom* general, Lachit Borphukan deployed his troops dressed as demons near the Mughal camps at night to terrorise the Mughal army during the famous battle of Saraighat is an exhibit from Assam's

[8] For more on this, read Sun Tzu's *Art of War* or Kautalya's *Arthashastra*



Lachit Borphukan deployed his troops dressed as demons near the Mughal camps at night to terrorise the Mughal army during the famous battle of Saraighat

martial history.[9] The Central Intelligence Agency's use of radio technology in the form of Radio Free Europe and Radio Liberty is a Cold War era demonstrations of using technology for propaganda.[10]

With the adoption of AI, the TVEs have added a vital element to their propaganda operations; scale. Scale in this context have multiple layers. Firstly, with AI-enabled technology, generation of content has become democratised. While in earlier days, content generation was the purview of a select few in the media cells of these TVEs, with the help of AI, virtually anybody could generate content to further their misinformation and influence campaigns. A November 2023 study by Tech Against Terrorism demonstrates how AI is being used by terror outfits like al Qaeda and Daish as well as Extreme Right-Wing groups alike.[11] Another February 2024

[9] Kumar, P., & Mishra, V. (2021). A Study of the Military Strategy and Leadership of Ahom Commander Lachit Barphukan. *INDIAN STUDIES REVIEW*, 35. and Khagen, G. (2017). Ahom warfare evolution nature and strategy. *Gauhati University.* http://hdl.handle.net/10603/224778.

[10] Johnson, A. R. (2018). Managing media influence operations: Lessons from radio free Europe/Radio liberty. *International Journal of Intelligence and CounterIntelligence*, *31*(4), 681-701.

[11] Tech Against Terrorism. (2023). Early terrorist experimentation

AI is being used by terror outfits like *al Qaeda* and *Daesh* as well as Extreme Right-Wing groups alike.

study examined AI generated contents by pro-*Daish* groups on four social media platforms, Instagram, Pinterest, Pixiv and Meta with a sample size of over 280 unique contents.[12] These studies point to the fact that content generation for furthering the ideologies of TVEs have gotten a definite fillip with the adoption of open-source AI-based technologies.[13]

Secondly, with the adoption of AI, TVEs have been able to generate better reach for their influence operations. This is especially true when they adopt NLP-based training models like Phonetic Models and Language Mapping,[14] Rule-based Systems,[15] Corpus Training,[16] Phonetic Algorithms,[17]

with generative artificial intelligence services. In *Tech Against Terrorism*. https://www.techagainstterrorism.org.

[12] Criezis, M. (2024). AI Caliphate: The creation of Pro-Islamic state propaganda using generative AI. *GNET*. https://gnet-research.org/2024/02/05/ai-caliphate-pro-islamic-state-propaganda-and-generative-ai/.

[13] Tech Against Terrorism. 5-6.

[14] Lee, D., Kim, D., Yun, S., & Kim, S. (2021). Phonetic Variation Modeling and a Language Model Adaptation for Korean English Code-Switching Speech Recognition. *Applied Sciences*, *11*(6), 2866. https://doi.org/10.3390/app11062866.

[15] Kovarik Jr, V. J. (2006). Cognitive research: Knowledge representation and learning. In *Cognitive Radio Technology* (pp. 365-399). Newnes.

[16] What is a Training Corpus?. *The AI Navigator.* https://www.theainavigator.com/blog/what-is-a-training-corpus.

[17] Vykhovanets, V. S., Du, J., & Sakulin, S. A. (2020). An overview of phonetic encoding algorithms. *Automation and Remote Control*, *81*, 1896-1910.

Tools like CAMeL and PyArabic on GitHub, Bhashini are some examples of such transliteration tools.

Contextual AI,[18] etc. While these may seem fairly complex methodologies, the TVE actor does not really need to know any of these critical and emerging technologies. All they need to do is leverage various open-source tools available for free to translate their text to multiple languages with high degree of accuracy, thus reach of their propaganda. Tools like CAMeL and PyArabic on GitHub,[19] Bhashini[20] are some examples of such transliteration tools.

Lastly, the speed of dissemination of propaganda is another aspect where AI has enabled these malicious actors to execute influence operations with ease. A relevant case in point would be the example of the hashtag hijacking of FIFA World Cup cited above where the LEAs were merely playing whack-a-mole and TVE actors operated at will.

[18] Brdiczka, O. (2019). Contextual AI-The Next Frontier Towards Human-Centric Artificial Intelligence. In *Machine Learning@ Georgia Tech Seminars* (pp. 02-28).

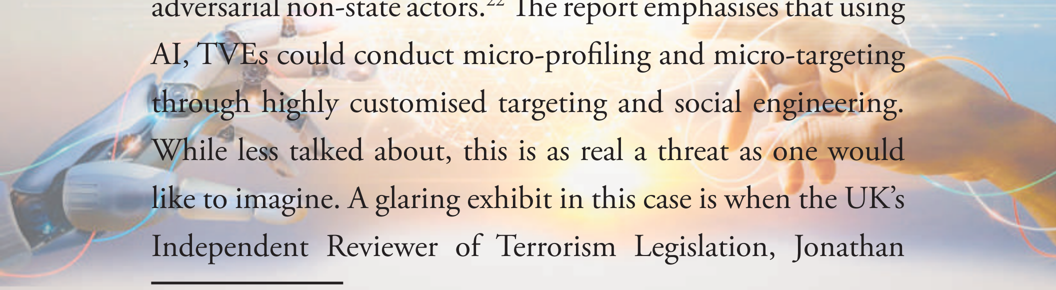
[19] Linuxscout. (n.d.). *pyarabic/paper.md at master · linuxscout/ pyarabic*. GitHub. https://github.com/linuxscout/pyarabic/blob/ master/paper.md.

[20] Bose, A. (2022). Explained: What is Bhashini and how it can bridge the gap between Indian languages. *The Times of India*. https://timesofindia.indiatimes.com/gadgets-news/explained-what-is-bhashini-and-how-it-can-bridge-the-gap-between-indian-languages/articleshow/93928335.cms#:~:text=The%20government%20of%20India%20has,tongues%20by%20using%20available%20technology.

UK's Independent Reviewer of Terrorism Legislation, Jonathan Hall was reportedly "recruited" by an AI bot into the terrorist folds.

Recruitment

The next aspect of TVEs' operation where AI-based technologies have been transformative is recruitment of fresh cadres into their ranks and file. This involves both identification of potential recruits as well as the actual act to acculturate them into the folds of the TVEs ideology, as espoused by scholar John Horgan.[21] A joint report published by the UNCCT & UNICRI in 2021 demonstrates how AI has been used to carry out these two aspects of recruitment by adversarial non-state actors.[22] The report emphasises that using AI, TVEs could conduct micro-profiling and micro-targeting through highly customised targeting and social engineering. While less talked about, this is as real a threat as one would like to imagine. A glaring exhibit in this case is when the UK's Independent Reviewer of Terrorism Legislation, Jonathan



[21] Horgan, J. (2008). From profiles to pathways and roots to routes: Perspectives from psychology on radicalization into terrorism. *The ANNALS of the American Academy of Political and Social Science*, *618*(1), 80-94.

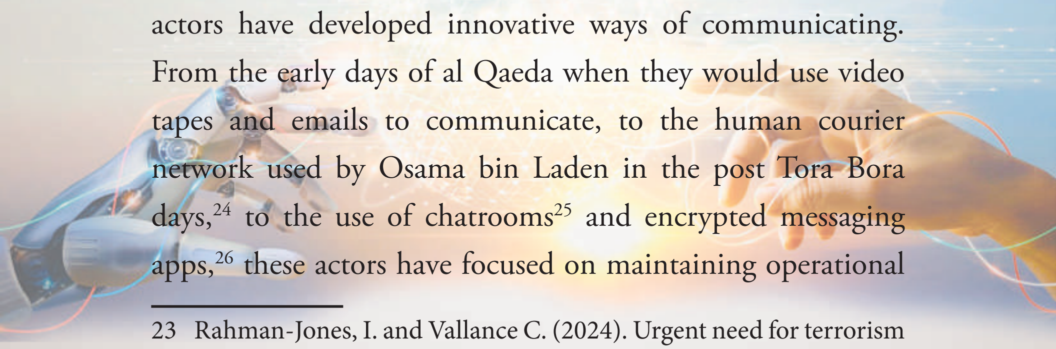
[22] Voronkov, V., & De Meo, A. M. (2021). Countering Terrorism Online With Artificial Intelligence. In *A Joint Report by UNICRI and UNCCT*. United Nations Office of Counter-Terrorism. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf.

> Post May 2020, *Hay'at Tahrir al Sham,* instructed its members to move away from conventional encrypted platforms like Telegram, Facebook Messenger, etc. to more bespoke and more advanced communication platforms like Conversations, SilentCircle, Redphone, and Signal.

Hall was reportedly "recruited" by an AI bot into the terrorist folds.[23]

Communication

Communication is the backbone of any organisation. TVEs are no different in this regard. Over the years, these threat actors have developed innovative ways of communicating. From the early days of al Qaeda when they would use video tapes and emails to communicate, to the human courier network used by Osama bin Laden in the post Tora Bora days,[24] to the use of chatrooms[25] and encrypted messaging apps,[26] these actors have focused on maintaining operational



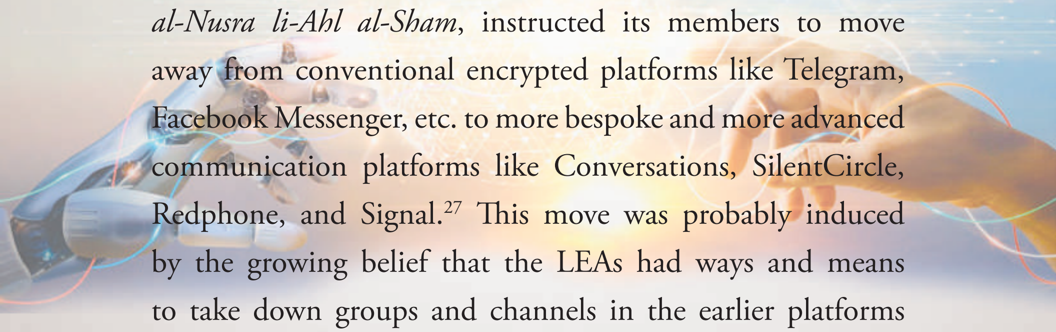
[23] Rahman-Jones, I. and Vallance C. (2024). Urgent need for terrorism AI laws, warns think tank. *BBC.* https://www.bbc.com/news/technology-67872767.

[24] DAHL, E. J. (2014). Finding Bin Laden: Lessons for a New American Way of Intelligence. *Political Science Quarterly*, *129*(2), 179–210. http://www.jstor.org/stable/43828649.

[25] Higgins, A., Leggett, K., & Cullison, A. (2002). How al Qaeda Put Internet in Service of Global Jihad. *Wall Street Journal*. https://www.wsj.com/articles/SB1036967366463939428.

[26] Bhattacharyya, R. (2022). Al-Qaida-Affiliated terrorists in India found with sophisticated communication app. *The Diplomat*.

The January 2025 issue of the Voice of Khurasan mentioned masseging applications like Signal, Threema, WhatsApp, Rocket Chat, Facebook Messenger, with comparative analysis among these applications based of geographic location of its operative, the communication goals, like recruitment, propaganda, operational planning, etc.



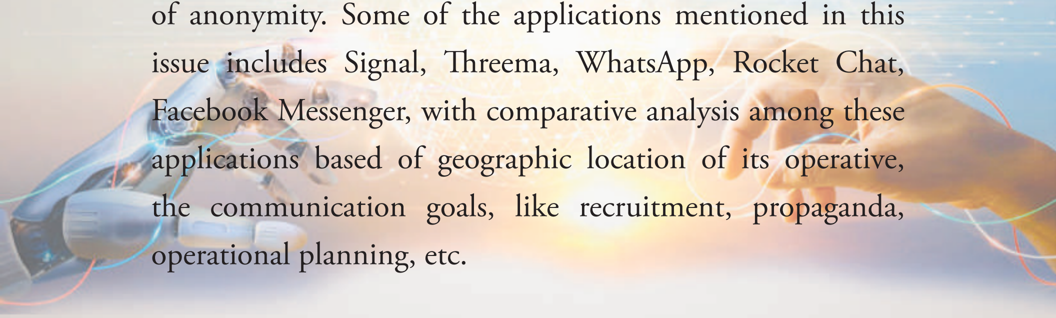
and communication security as core focus. With the advent of COVID-19, these organisations have heavily leveraged on advanced and sometimes bespoke platforms to communicate. For instance, it was seen that post May 2020, *Hay'at Tahrir al Sham,* formerly *Jabhat Fatah al-Sham* and prior to that *Jabhat al-Nusra li-Ahl al-Sham*, instructed its members to move away from conventional encrypted platforms like Telegram, Facebook Messenger, etc. to more bespoke and more advanced communication platforms like Conversations, SilentCircle, Redphone, and Signal.[27] This move was probably induced by the growing belief that the LEAs had ways and means to take down groups and channels in the earlier platforms like Telegram.[28] Also, the actions of online hacktivist groups

https://thediplomat.com/2022/08/al-qaida-affiliated-terrorists-in-india-found-with-sophisticated-communication-app/.

[27] Awasthi, S. (2024). The dark web as enabler of terrorist activities. *Observer Research Foundation*. https://www.orfonline.org/research/the-dark-web-as-enabler-of-terrorist-activities.

[28] Schectman, J., Schechner, S. and Cullison, A. (2024). How Telegram Became a Hunting Ground for Criminals—and Cops. *The Wall*

like Anonymous in the aftermath of 2015 Paris attacks when the group took down over 25,000 *Daesh* accounts, may have been a strong incentive for such shift to higher end communication platforms.[29] The busting of scores of al Qaeda affiliated sleeper cells in India in 2022-23 also witnessed this phenomenon where it was reported that these TVE actors used highly sophisticated messaging applications.[30] The January 2025 issue of the Voice of Khurasan, an Islamic State in Khurasan Province (ISKP) mouthpiece, dedicates an entire chapter named "Light of Darkness" on various open-source encrypted messaging applications which may be leveraged by their followers. It details out the steps to be followed to use each of these messaging applications to add further layers of anonymity. Some of the applications mentioned in this issue includes Signal, Threema, WhatsApp, Rocket Chat, Facebook Messenger, with comparative analysis among these applications based of geographic location of its operative, the communication goals, like recruitment, propaganda, operational planning, etc.



Street Journal. https://www.wsj.com/tech/how-telegram-became-a-hunting-ground-for-criminalsand-cops-8195f483.

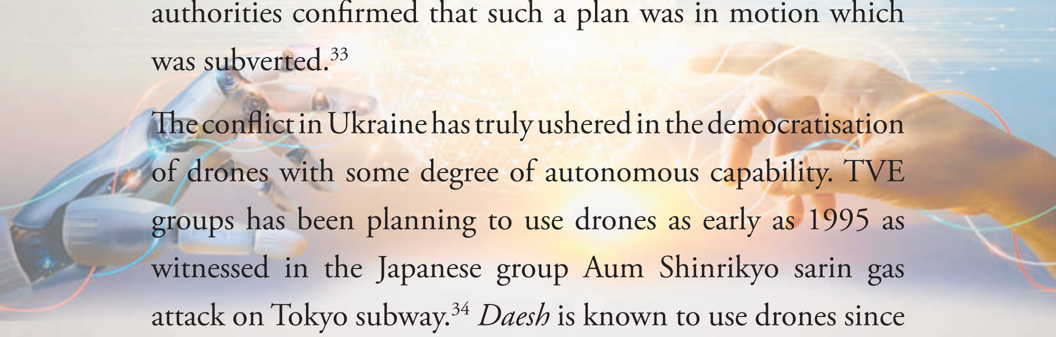
[29] UNICRI and UNCCT. (2021). Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes.

[30] Kalita, P. (2022). Islamic terror groups using sophisticated apps: Assam CM Himanta Biswa Sarma. *The Times of India*. https://timesofindia.indiatimes.com/city/guwahati/islamic-terror-groups-using-sophisticated-apps-assam-cm-himanta-biswa-sarma/articleshow/93359091.cms.

> *Daesh* had released a video showcasing a self-drive vehicle with mannequins to boast about their ability to use driverless cars to conduct bomb attacks.

Attack Planning & Execution

A January 2024 study of the Combating Terrorism Center at Westpoint demonstrates how AI can be leveraged for attack planning and how the guardrails and content moderation mechanisms of popular generative AI platforms prove inadequate at best to prevent such usage.[31] As early as 2016, *Daesh* had released a video showcasing a self-drive vehicle with mannequins to boast about their ability to use driverless cars to conduct bomb attacks.[32] In 2018, British authorities confirmed that such a plan was in motion which was subverted.[33]



The conflict in Ukraine has truly ushered in the democratisation of drones with some degree of autonomous capability. TVE groups has been planning to use drones as early as 1995 as witnessed in the Japanese group Aum Shinrikyo sarin gas attack on Tokyo subway.[34] *Daesh* is known to use drones since

[31] Weimann, G., Pack, A. T., Sulciner, R., Scheinin, J., Rapaport, G and Diaz, D. (2024). Generating Terror: The risks of Generative AI exploitation. *Combating Terrorism Center at West Point*. https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation/.

[32] Algorithms and terrorism.

[33] Ibid.

[34] Rassler, D. (2016). Remotely piloted innovation: terrorism, drones and supportive technology. *Combating Terrorism Center at West*

2016 as well. Similarly, al Qaeda in Arabian Peninsula had claimed responsibility of at least seven attacks on the Shabwa Defense Forces in South Yemen between May and July 2023. Thus, it will not be a leap to expect TVEs to use AI-enabled autonomous vehicles (cars, drones, sub-surface vehicles, etc.) to carry out attacks. This assertion can be validated by the 2019 report by the Global Counterterrorism Forum, titled *Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems.*[35] Closer to home, there have been several reports of drones being used by insurgent groups in the ongoing conflict in Manipur.[36]

Another use of AI in planning and executing attacks is in the cyberspace. TVEs have long boasted about their capabilities to launch large scale, crippling cyber-attacks. Though empirical evidence in this regard is scant at the moment, a 2018 report published as a joint project among eminent scholars and industry experts outlined cyber-attacks as a potential threat vector to be leveraged by TVEs.[37] As latest as December 2024,

Point. https://apps.dtic.mil/sti/pdfs/AD1019773.pdf.

[35] Bushehri, F. (2021). Good practices: Countering terrorist use of unmanned aerial systems. *The GCTF*. https://www.thegctf.org/Resources/Interactive-Content/Videos/ArtMID/802/ArticleID/173/Good-Practices-Countering-Terrorist-Use-of-Unmanned-Aerial-Systems.

[36] Singh, V. (2024). Manipur drone attack: Looted ammunition said to have been used. *The Hindu*. https://www.thehindu.com/news/national/manipur/drones-used-in-manipur-violence-may-have-been-assembled-locally/article68602252.ece.

[37] Participants in the Expert Group Meeting included representatives

al Qaeda operatives arrested in India were seen to be leveraging AI and other advanced communication technologies to plan, coordinate and execute physical attacks.

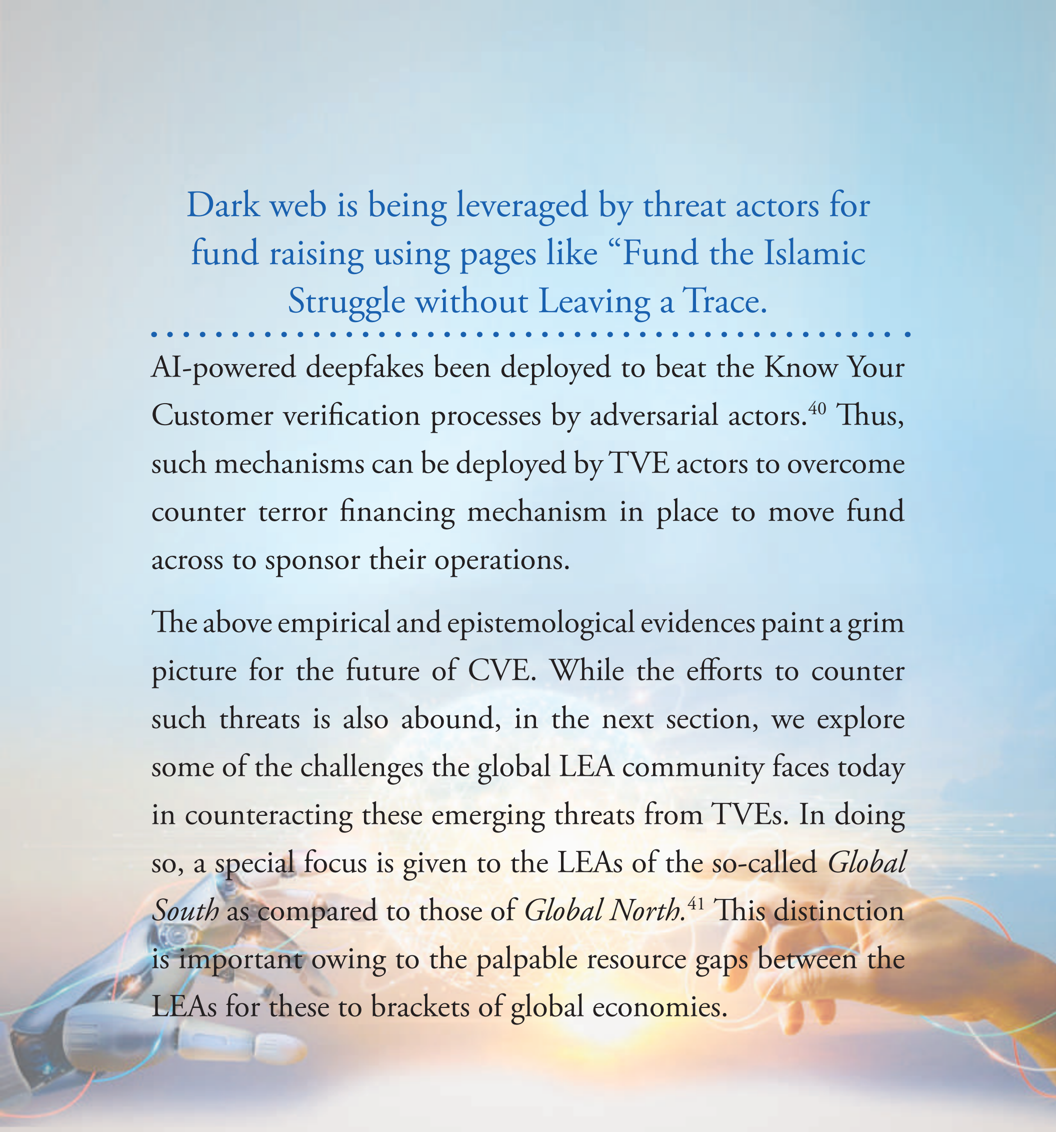
Terror Financing

While terror financing has seen many novel tactics, techniques and procedures, the use of AI based technologies and cryptocurrencies is the latest innovation. TVEs are known to have been leveraging dark web and cryptocurrencies to fund their operations. The US Department of Treasury has reported that dark web is being leveraged by threat actors for fund raising using pages like "Fund the Islamic Struggle without Leaving a Trace."[38] Evidences of cryptocurrencies been used to finance the 2015 Paris Attack and the 2021 Easter Bombing in Sri Lank has also come to fore.[39] Reports also assets that

from: AWO; Infinium Robotics; INSIKT Intelligence; INTERPOL; LIRNEasia; Omdena Inc.; SIMAVI; the Cyber Security Cooperative Research Centre; the Department of Research and Innovation, Ministry of Education, Myanmar; the Digital Rights Foundation, Pakistan; the Graduate Institute of International and Development Studies, Geneva; the Home Team Science and Technology Agency (HTX), Singapore; the Human Rights Commission of Malaysia (SUHAKAM); the Indian Police Service; the Information and Technology Division, Sri Lankan Police; the Police Policy Research Center, National Police Agency, Japan; the S. Rajaratnam School of International Studies (RSIS), Singapore; the Southeast Asia Regional Centre for Counter Terrorism (SEARCCT); the University of Tokyo, Japan; and Tisane Labs.

[38] Department of the Treasury. (2024). 2024 National Terrorist Financing Risk Assessment. https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf.

[39] Algorithms and terrorism.



> Dark web is being leveraged by threat actors for fund raising using pages like "Fund the Islamic Struggle without Leaving a Trace.

AI-powered deepfakes been deployed to beat the Know Your Customer verification processes by adversarial actors.[40] Thus, such mechanisms can be deployed by TVE actors to overcome counter terror financing mechanism in place to move fund across to sponsor their operations.

The above empirical and epistemological evidences paint a grim picture for the future of CVE. While the efforts to counter such threats is also abound, in the next section, we explore some of the challenges the global LEA community faces today in counteracting these emerging threats from TVEs. In doing so, a special focus is given to the LEAs of the so-called *Global South* as compared to those of *Global North.*[41] This distinction is important owing to the palpable resource gaps between the LEAs for these to brackets of global economies.

[40] Urgent need for terrorism AI laws.

[41] Kenny, M. (2025). Global North and Global South | Definition, Countries, differences, history, map, & Facts. *Encyclopedia Britannica*. https://www.britannica.com/topic/Global-North-and-Global-South.

Challenges to Counter AI-enabled TVE Actors for the Global South

The division of the world between the Global North and South is largely based on economic grounds. As such, the challenges faced by the LEAs of these two factions also stems from their budgetary allocations. A comparative analysis of the internal security budget of the states of these two groupings of the world are depicted in Table 1 below. The table demonstrates how over a period of last five years, between 2019 to 2024, the gap in internal security budgetary allocation has evolved in these two economic hemispheres of the world.

INTERNAL SECURITY BUDGETS							
Group	Country	Years, followed by amount in Billion USD					
		2019	2020	2021	2022	2023	2024
G7	Canada	1.2	1.27	1.35	1.42	1.5	1.58
	France	3.41	3.52	3.63	3.74	3.85	3.96
	Germany	2.75	2.86	2.97	3.08	3.19	3.3
	Italy	1.65	1.76	1.87	1.98	2.09	2.2
	Japan	9	9.75	10.5	11.25	12	12.75
	UK	1.75	1.88	2	2.12	2.25	2.38
	USA	60.4	61.5	62.6	63.7	64.8	65.9

INTERNAL SECURITY BUDGETS							
G20	India	14	19.7	19.6	21.8	23.9	25.8
	Argentina	3.13	2.83	3.07	2.58		
	Australia	1.2	1.3	1.4	1.5	1.6	1.7
	Brazil	25.91	19.59	19.19	20.21		
	China	240.3	258	285.9	292	203	231.4
	Indonesia	8.15	9.39	8.8	8.99		
	Mexico	11.4					
	Russia	32.1	36.5	41.2	45.8	50.3	55.1
	Saudi Arabia	60.8	66.1	71.7	71.7	69	71.7
	South Africa	3.44	3.23	3.39	3.00		
	South Korea	36.21	39.4	42.3	46.12	46.85	50
	Turkey	10.64	10.69	10.58	10.55	10.6	10.64
Others	Sri Lanka	1.05	1.1	1.15	1.2	1.25	1.3
	Bangladesh	3.74	4.51	5.17	4.65	4.1	
	Malaysia	3.27	3.37	3.68	3.67	4.3	4.3
	Thailand	5.72	5.89	6.06	5.89		
	Israel	2.4	2.5	2.6	2.7	2.8	2.9
	Egypt	3.74	4.51	5.17	4.65		

Table 1: *Internal Security Budget Allocation Comparison from 2019-2024 as per official announcements of the countries.*

Emanating out of this economic disparity, the challenges faced by the LEAs of the states with limited access to internal security budget are also unique. The some of these are detailed below. While some of these challenges may be pertinent to the more prosperous LEAs as well, addressing them is relatively easier for them as a greater percentage of their budget can be allocated to address these challenges and resolve them at a faster rate. For the purpose of this paper, we shall investigate these challenges from the vantage point of the lesser prosperous LEAs of the Global South. The challenges of LEAs range from policy level roadblocks to tactical challenges of resource availability and data integrity. Some of the salient points in this regard are discussed below.

Digitisation of Data

To take advantage of technological advancements, the first step is to have data available in a digitised format. The primary source of data for many LEAs still remains in physical form. Even where there is digitisation, the focus of such initiatives has largely remained to be record keeping and such data is difficult to use for tech driven decision making. A primary reason for that has been the policy level hesitation owing to the triad of Confidentiality, Integrity and Availability (CIA) of cybersecurity.[42] Most of these data remains classified and unauthorised access to such data may wreak havoc from a national security standpoint. Also, maintaining the integrity of data at a data entry stage also poses a major challenge. A case in point here would be the mission mode digitisation project launched by the Government of India in 2009, christened as Crime and Criminal Tracking and Network

[42] Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., & Sweetnam, J. (2020). Data integrity: Detecting and responding to ransomware and other destructive events (No. NIST Special Publication (SP) 1800-26 (Withdrawn)). N*ational Institute of Standards and Technology.*

Systems (CCTNS).[43] While the project has been live all across the nation, the quality of data ingested at the last mile remains under critique and scrutiny by the country's principal accounting authority, Comptroller and Auditor General of India.[44] Even when flawless digitisation is achieved, making such data available to end users has both technological and policy challenges within the Indian legal framework owing to the much-feared Official Secrets Act of 1923.[45]

Democratisation of Data

Digital, machine-readable data is available within certain institutional frameworks in some cases. In the Indian context, institutions like Indian Cybercrime Coordination Centre (I4C),[46] NatGrid,[47] CriMAC,[48] etc. are some examples.

[43] Digital Police (n.d.). Crime and Criminal Tracking Network & Systems (CCTNS). *Ministry of Home Affairs, India*. https://digitalpolice.gov.in/DigitalPolice/AboutUs.

[44] Compliance Audit on "Implementation of Crime & Criminal Tracking Network Systems (CCTNS)" (2020). *Comptroller and Auditor General of India*. https://cag.gov.in/uploads/icisa_it_reports/Assam-CCTNS-064f1c642c9a136-90462975.pdf.

[45] Deepalakshmi, K. (2023). All you need to know about the Official Secrets Act. *The Hindu.* https://www.thehindu.com/news/national/all-you-need-to-know-about-the-official-secrets-act/article61575198.ece.

[46] Indian Cybercrime Coordination Centre. *Ministry of Home Affairs, India*. https://i4c.mha.gov.in/.

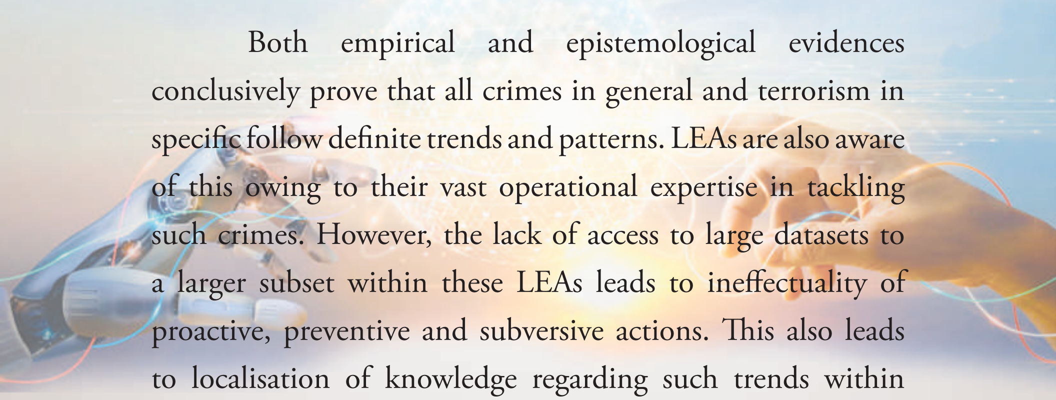
[47] Understanding NATGRID - India's National Intelligence grid. *The Geostrata*. https://www.thegeostrata.com/post/understanding-natgrid-india-s-national-intelligence-grid.

[48] Singh, V. (2022). Seven States cold to Centre's crime portal. *The Hindu*. https://www.thehindu.com/news/national/some-states-

> The lack of access to large datasets to a larger subset within these LEAs leads to ineffectuality of proactive, preventive and subversive actions.

However, ownership of such data and bureaucratic red tapes as to sharing of such data within a larger stakeholder base acts as major barriers to access. While there are legitimate reasons for not sharing data by these institutions more broadly, this leads to stifling of operational and tactical capabilities at a more localised level.

Inability to take a proactive approach



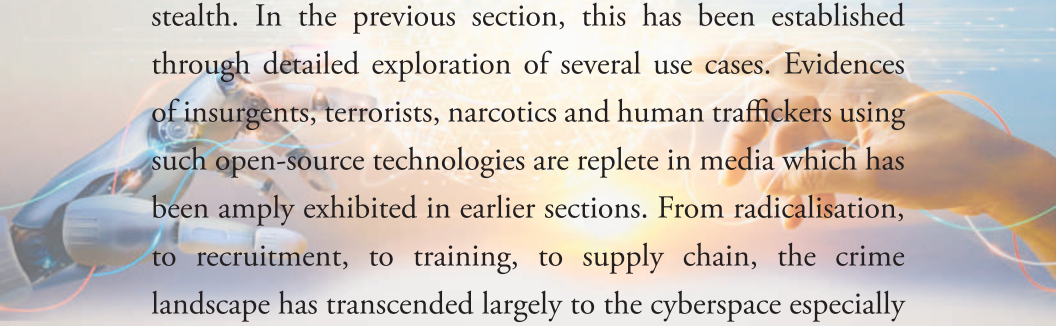
Both empirical and epistemological evidences conclusively prove that all crimes in general and terrorism in specific follow definite trends and patterns. LEAs are also aware of this owing to their vast operational expertise in tackling such crimes. However, the lack of access to large datasets to a larger subset within these LEAs leads to ineffectuality of proactive, preventive and subversive actions. This also leads to localisation of knowledge regarding such trends within a few subject matter experts (SMEs) within the LEAs. This transcends into challenges of transferability of knowledge owing to both human and organisational lacunas.

give-cold-shoulder-to-centres-portal-to-share-info-on-crimes/article65836345.ece.

> From radicalisation, to recruitment, to training, to supply chain, the crime landscape has transcended largely to the cyberspace especially in the post COVID world.

Evolving modus operandi within typologies of crime

As TVEs, unlike the LEAs, are not restricted by laws, policies, procedures and rules, they are able to adopt rapidly evolving technologies to further their criminal enterprise at scale. Also, open-source availability of such technologies as well as proliferation of ungoverned social media space gives these elements an almost unrestricted ability to operate with stealth. In the previous section, this has been established through detailed exploration of several use cases. Evidences of insurgents, terrorists, narcotics and human traffickers using such open-source technologies are replete in media which has been amply exhibited in earlier sections. From radicalisation, to recruitment, to training, to supply chain, the crime landscape has transcended largely to the cyberspace especially in the post COVID world.



Challenge of expertise

While the LEAs are rich in their experience in matters of crime prevention and law enforcement, the ability to develop, adopt and democratise CET at scale is lacking. Notwithstanding pockets of excellence within the LEAs, leveraging on such expertise in a repeatable manner faces organisational and operational challenges.

Unavailability of holistic and contextual solutions

LEAs have been making progress in adopting technology through procurement of point solutions focused at one or the other aspects of digital augmentation. However, such off-the-shelf solutions do not address the challenges of the LEAs with a holistic approach. Such solutions generally operate in isolation and more often than not, work in silos. This leads to lack of ability of LEAs to derive actionable intelligence for proactive and preventive approaches to discharging their core mandate.

Lack of diversity of data

Though digital platforms have been deployed for predictive preventive action by LEAs, such systems are generally hampered by the quality of input data which is generally unidimensional or at best two-dimensional, as in the case of Crime Mapping Analytics and Predictive System (CMAPS) as deployed in the Indian state's capital of New Delhi.[49] CMAPS is known to layer its predictive model on a dataset sourced from Dial 100 emergency response system and CCTNS. This limits the system into a linear decision-

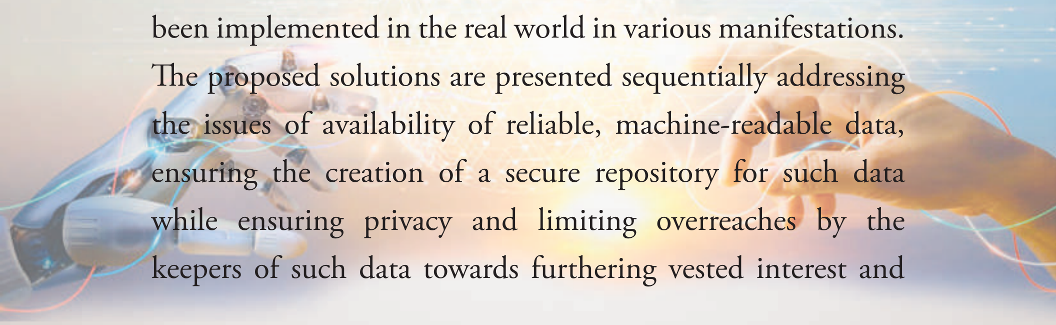
[49] Choudhary, L. (2024). Predictive policing is dumb. *Analytics India Magazine*. https://analyticsindiamag.com/predictive-policing-is-dumb/.

making loop as it does not factor in huge cache of social, natural, geographical and historical factors which may trigger criminal behavior.

The above exploration of challenges faced by LEAs of the Global South and with empirical evidences from India, which is sometimes coined as the leader of the Global South, the paper posits that a reasonably strong conceptual foundation has been established in this section. In the next section, we thrive to explore how CET like AI and its sub-streams are useful to counter these challenges in a low-cost, high-yield scenario. While some of these solutions may leverage on academic studies, real life implementations of these are already achieved in the more prosperous avenues of the world.

Leveraging CET to Counter AI-enabled Threats from TVEs

In this section, we shall explore practicable application of CET in addressing the challenges posed by the TVEs especially in the post COVID world. In the ensuing sub-sections, we shall propose some of the solutions which have proven applicability with strong academic foundation and has also been implemented in the real world in various manifestations. The proposed solutions are presented sequentially addressing the issues of availability of reliable, machine-readable data, ensuring the creation of a secure repository for such data while ensuring privacy and limiting overreaches by the keepers of such data towards furthering vested interest and

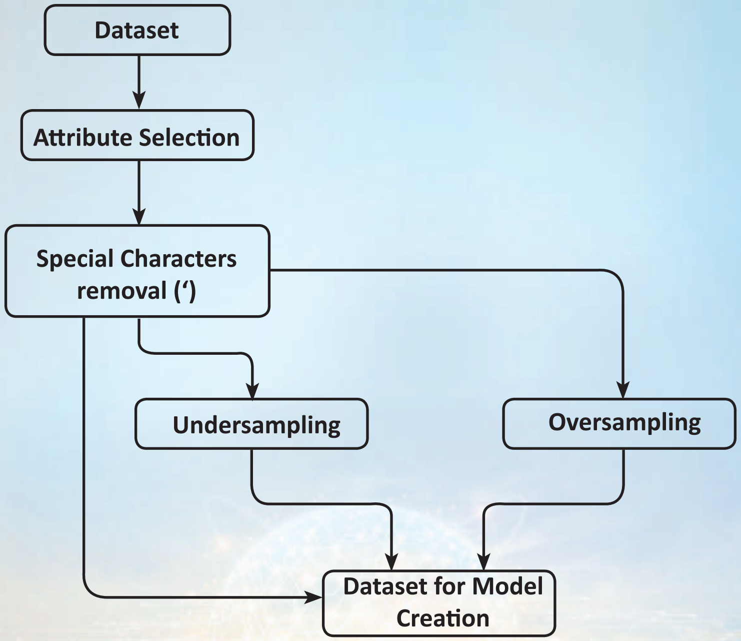


The proposed solutions are presented sequentially addressing the issues of availability of reliable, machine-readable data, ensuring the creation of a secure repository for such data while ensuring privacy and finally processing the data to generate actionable intelligence finally processing the data to generate actionable intelligence which would enable LEAs to take preventive measures against TVEs. While the underlying technologies in each of these cases are discussed in some details in this section, the primary focus is to use such advanced technologies to address the growing challenge of TVE groups themselves leveraging such technologies to further their reprehensible schemes.

The first step in formulating a technological architecture is to ensure flawless, machine-readable data which forms the backbone of any solution. In order to ensure integrity of the data, machine enabled data pre-processing may be a practicable approach to mitigate against data-entry errors. This is required to clean the data and transform it into understandable structures which involves four steps; data cleaning, data integration, data transformation and data reduction. This is critical especially when multi-source input mechanisms are used to generate the master database.[50] Fig. 1 demonstrates this process pictorially.

Once a reliable mechanism is in place using the above process, the next step is to ensure the data repository is secure while addressing legitimate privacy concerns. To ensure the confidentiality of digitised data, the author submits that the envisioned database be protected using cutting-edge

[50] Gundabathula, V. T., & Vaidhehi, V. (2018). An efficient modelling of terrorist groups in India using machine learning algorithms. *Indian Journal of Science and Technology*, *11*(15), 1-10.



TrustTech solutions like Fully Homomorphically Encrypted (FHE)[51] environments with a layer of Searchable Symmetric Encryption (SSE).[52] These two encryption solutions are described by US’s DARPA as the “perfect balance between privacy and security” and is deployed for sensitive databases in the US.[53] This combination, according to the author, would

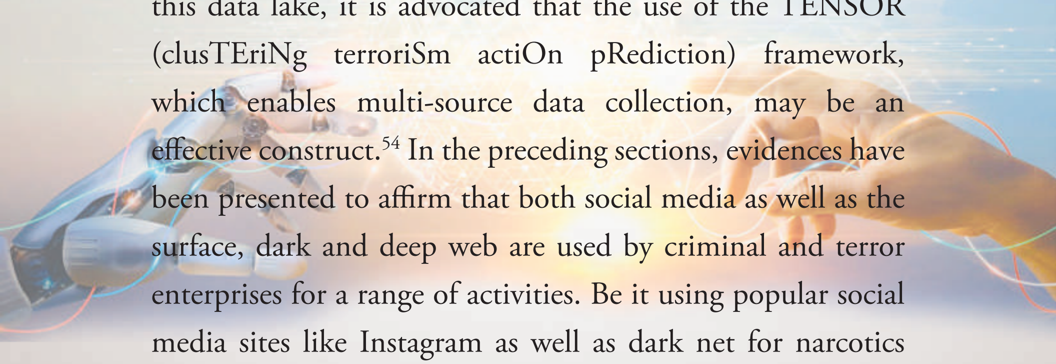
[51] Marr, B. (2021). What is homomorphic encryption? and why is it so transformative? *Forbes*. https://www.forbes.com/sites/bernardmarr/2019/11/15/what-is-homomorphic-encryption-and-why-is-it-so-transformative/?sh=71f02727e939.

[52] Arampatzis, A. (2024). What is Searchable Symmetric Encryption?. *Venafi, a CyberArk Company*. https://venafi.com/blog/what-searchable-symmetric-encryption/.

[53] DARPA (2023). DARPA selects researchers to accelerate use of fully homomorphic encryption. *DARPA.* https://www.darpa.mil/news-

These two encryption solutions are described by US's DARPA as the "perfect balance between privacy and security"

ensure that the stored data is not accessible in its primary form to the users who can run analysis on these datasets within the encrypted environment and only the output is accessible to the user.



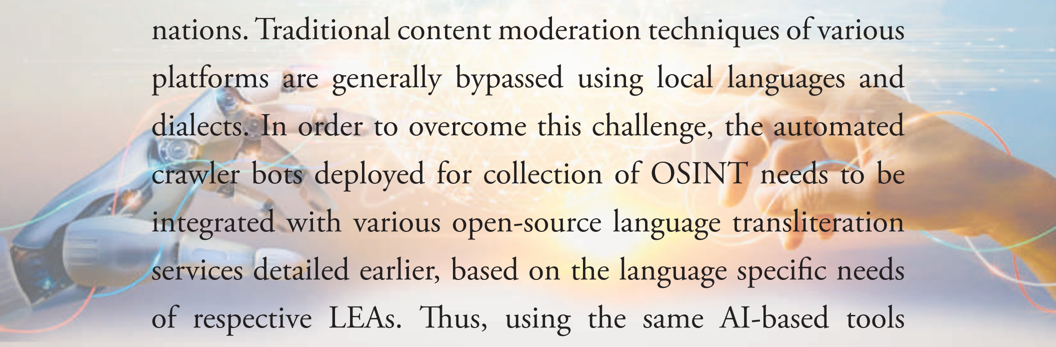
Once the above approach is applied to generate accurate data and to store such data in a reliable and responsible manner, the next step is to formulate an all-source data collection strategy in order to operationalise such a data lake. While developing this data lake, it is advocated that the use of the TENSOR (clusTEriNg terroriSm actiOn pRediction) framework, which enables multi-source data collection, may be an effective construct.[54] In the preceding sections, evidences have been presented to affirm that both social media as well as the surface, dark and deep web are used by criminal and terror enterprises for a range of activities. Be it using popular social media sites like Instagram as well as dark net for narcotics trade, illegal weapons trade, human trafficking, etc. or for propaganda dispensation and recruitment by terrorist and insurgent groups using Facebook, Twitter, etc., TVE elements

events/2021-03-08.

[54] Sormani, R., Archetti, F., & Giordani, I. (2017). Criticality assessment of terrorism related events at different time scales. *Journal of Ambient Intelligence and Humanized Computing*, *8*(1), 9-27.

The challenge that needs solving in this instance is to address the use of non-English languages, which is especially a point of concern for the Global South nations. Traditional content moderation techniques of various platforms are generally bypassed using local languages and dialects.

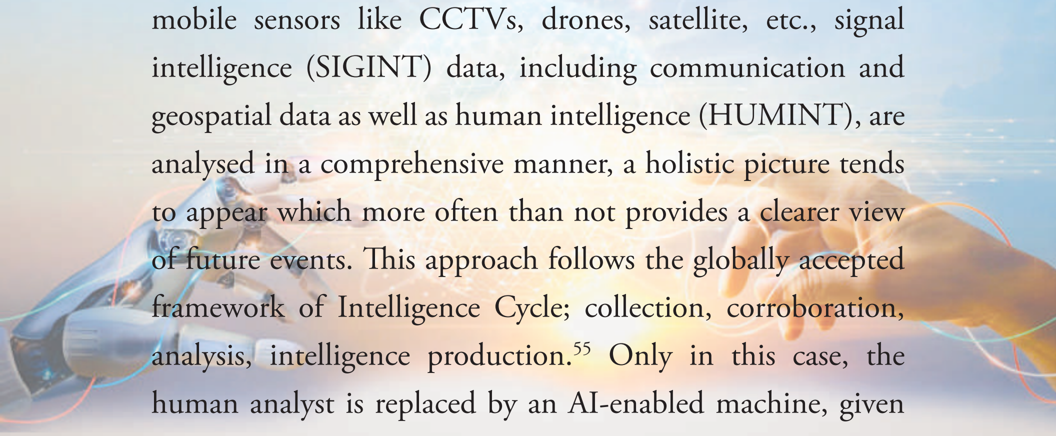
leverage modern communication and social media platforms to execute their unholy designs. Thus, collection of open-source intelligence (OSINT) in an automated manner is a common practice. However, the challenge that needs solving in this instance is to address the use of non-English languages, which is especially a point of concern for the Global South nations. Traditional content moderation techniques of various platforms are generally bypassed using local languages and dialects. In order to overcome this challenge, the automated crawler bots deployed for collection of OSINT needs to be integrated with various open-source language transliteration services detailed earlier, based on the language specific needs of respective LEAs. Thus, using the same AI-based tools deployed by the TVEs could be deployed to hunt them down.



Apart from OSINT, most governments have in place various structured data collection mechanism for various administrative and other purposes. Such data may include vehicle registration data, traffic data, crime and criminal data, voter or citizen records data, financial transaction data,

> OSINT, IMINT, IMINT, SIGINT, HUMINT are analysed in a comprehensive manner, a holistic picture tends to appear which more often than not provides a clearer view of future events.

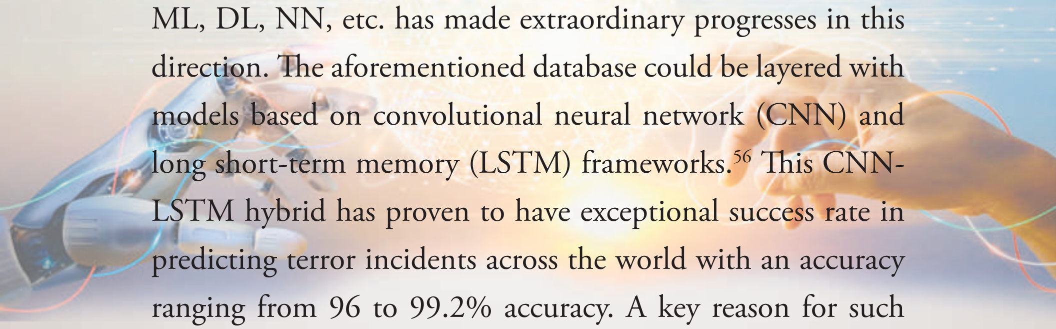
travel data, to name a few. In most states of the Global South though, such data resides in silos and are seldom integrated. The backdrop to this maybe technological or resource handicap as well as bureaucratic red tapes. However, when such data, in conjunction with other datasets like OSINT data, imagery intelligence (IMINT) data from static and mobile sensors like CCTVs, drones, satellite, etc., signal intelligence (SIGINT) data, including communication and geospatial data as well as human intelligence (HUMINT), are analysed in a comprehensive manner, a holistic picture tends to appear which more often than not provides a clearer view of future events. This approach follows the globally accepted framework of Intelligence Cycle; collection, corroboration, analysis, intelligence production.[55] Only in this case, the human analyst is replaced by an AI-enabled machine, given the sheer quantum of the data which may be analysed in this approach. This does not mean the role of the human analyst is obsolete and machines would be replacing them. This paper strongly backs the "man in the middle" approach of deploying



[55] The intelligence cycle. *Federation of American Scientists*. https://irp.fas.org/cia/product/facttell/intcycle.htm.

> CNN-LSTM hybrid has proven to have exceptional success rate in predicting terror incidents across the world with an accuracy ranging from 96 to 99.2% accuracy.

AI in decision making.



Once the aforementioned capabilities are developed, the LEAs would have at their disposal a holistic and secure all-source data lake which would then be leveraged to draw insights and arrive at fairly accurate predictions, given the diverse nature of the base data. Such actionable intelligence can only be produced, with the resource restrictions highlighted earlier, through the deployment of CET. Research in the fields of AI, ML, DL, NN, etc. has made extraordinary progresses in this direction. The aforementioned database could be layered with models based on convolutional neural network (CNN) and long short-term memory (LSTM) frameworks.[56] This CNN-LSTM hybrid has proven to have exceptional success rate in predicting terror incidents across the world with an accuracy ranging from 96 to 99.2% accuracy. A key reason for such phenomenal result is that this model incorporates multi-dimensional markers. The CNN model learns from the local features of the data-sets and the LSTM model extracts the context-dependent features to improve the overall accuracy of

[56] Saidi, F., & Trabelsi, Z. (2022). A hybrid deep learning-based framework for future terrorist activities modeling and prediction. *Egyptian Informatics Journal*, *23*(3), 437-446.

the model. Fig. 2 demonstrates the process pictorially.

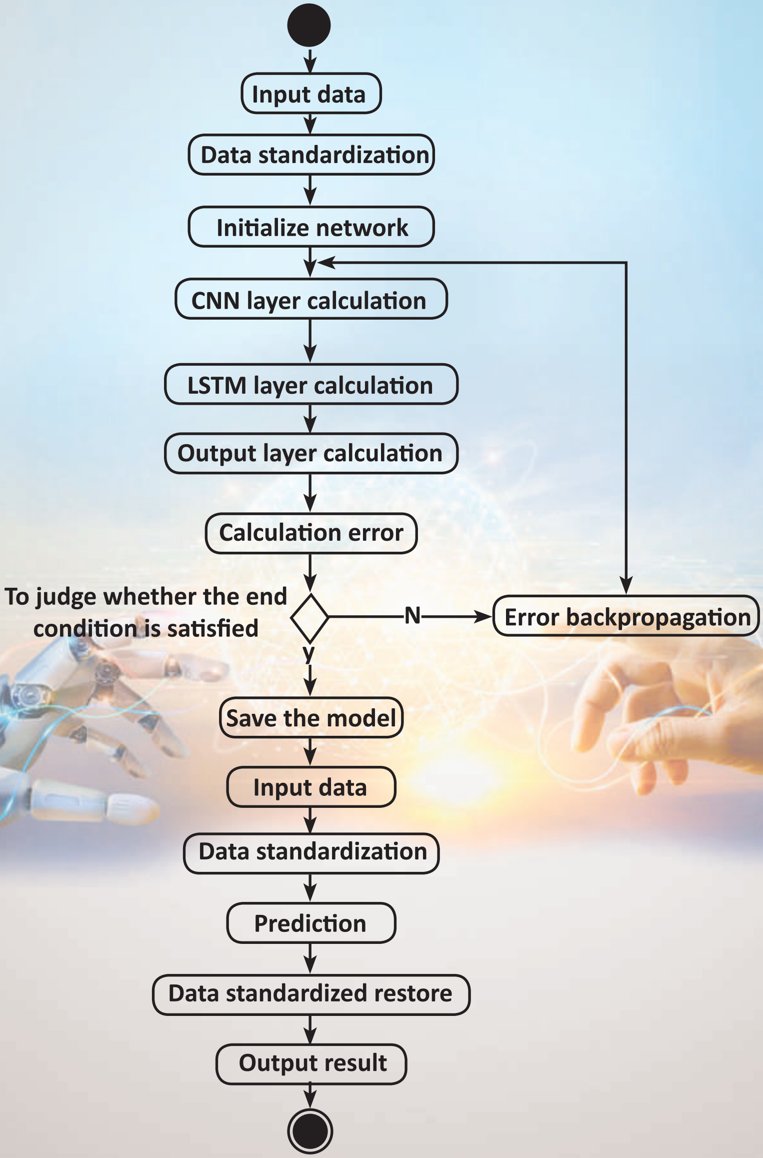
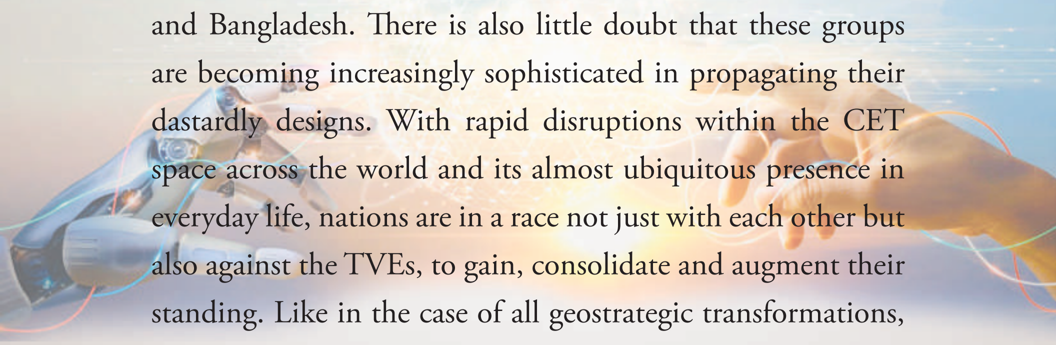


Figure 2: Hybrid CNN-LSTM model

Thus, the above exposition demonstrates how, by leveraging CET, LEAs of the Global South may be able to not just combat TVEs, but also outplay them in their own game through innovation, jointness of action and policy focus on farming the best possible outcome to derive actionable intelligence in their CVE missions.



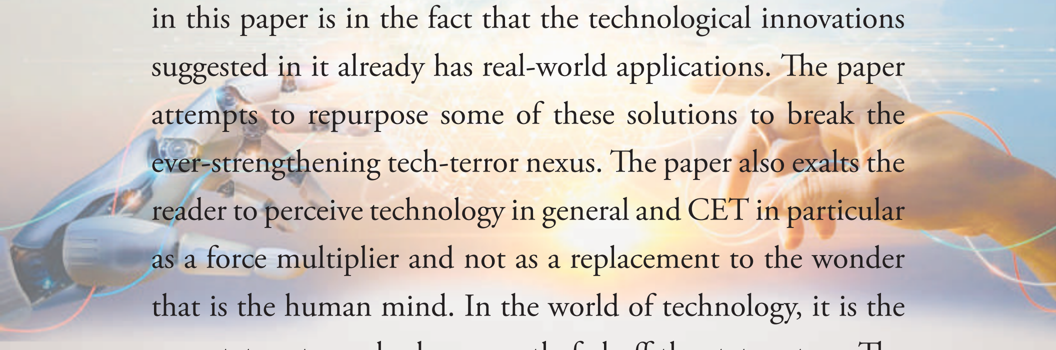
Conclusion

As uncertainties in geopolitics continue around the world, the threat from TVEs would continue to persist. This is because, such fluid global situation, coupled with raging conflicts, provide fertile base for propaganda, recruitment and attacks by TVEs. Exhibits of this is seen in West Asia as well as Russia and South Asia, including India, Pakistan and Bangladesh. There is also little doubt that these groups are becoming increasingly sophisticated in propagating their dastardly designs. With rapid disruptions within the CET space across the world and its almost ubiquitous presence in everyday life, nations are in a race not just with each other but also against the TVEs, to gain, consolidate and augment their standing. Like in the case of all geostrategic transformations, this puts the nation-states of the Global South in a perceived disadvantageous position. However, since technology is at the

Such fluid global situation, coupled with raging conflicts, provide fertile base for propaganda, recruitment and attacks by TVEs.

The paper also exalts the reader to perceive technology in general and CET in particular as a force multiplier and not as a replacement to the wonder that is the human mind.

base of this transformation, it adds a layer of normalisation, as it seeks human innovation over other resources, as proven in the case of DeepSeek by China. Innovators, policymakers, CVE professionals and technocrats would do well in considering the practicable and proven solutions highlighted in this paper to counter the ever-present threat from TVEs, while bridging the gaps between the 'haves' and 'have nots' in the community of nations. A key feature of the propositions recommended in this paper is in the fact that the technological innovations suggested in it already has real-world applications. The paper attempts to repurpose some of these solutions to break the ever-strengthening tech-terror nexus. The paper also exalts the reader to perceive technology in general and CET in particular as a force multiplier and not as a replacement to the wonder that is the human mind. In the world of technology, it is the non-state actors who have mostly fed off the state actors. The core assertion of the paper is to reverse the trend and beat the TVEs in their own game by feeding off their innovations and turning using such novelties in the CVE campaign of the Global South.



SHARE MEMBERS

Chairperson: The Chairperson shall provide overall leadership, guide strategic direction and organisational priorities and represent the organisation at high-level forums. They shall lead policy development, engage in advocacy efforts and liaison with government and key stakeholders. **Shri Radha Krishna Mathur,** former IAS Officer (batch of 1977) shall preside as the Chairperson of the organisation. Shri Mathur was the first Lieutenant Governor of Ladakh from 2019 to 2023. He was also the Chief Information Commissioner prior to heading the UT of Ladakh. He served the Govt. of Tripura for about 15 years and was the Chief Secy. of the state before joining Government of India where he served as the Secy. of MSME, Secy. of Defence Production and finally as the Defence Secy. of the Govt. of India. His contribution to the modernisation of the Indian Armed Forces is widely recognised both nationally and internationally. In Tripura, several path breaking initiatives were taken by him.

Vice Chairperson: Lt. Gen RP Kalita (Retd) Former General Officer Commanding, Eastern Command, Indian Army, is the Vice Chairperson of SHARE. Lt. Gen. Kalita, PVSM, UYSM, AVSM, SM, VSM (retd) has served for four decades the Indian Army in almost all its operational spectrums ranging from counter insurgency operations (COIN), to leading a Mountain Brigade, an Infantry Division, and a Corp. in NEI before taking charge as GOC-in-C, Eastern Command. He has had two tenures with the UN to Sierra Leone and Sudan. He is widely respected for his doctrinal depth on strategic affairs. He shall assist the Chairperson and shall lead all specific projects and initiatives related to defence and security.

General Secretary: The General Secretary will manage the operations while overseeing implementation of programs across the organisation, ensuring alignment with organisational objectives. **Shri Bhaskar J Mahanta,** IPS (Retd), former DGP Assam, (HoPF) and the Chief Information Commissioner Assam, is the current General Secretary of SHARE. A highly decorated officer, he is widely acknowledged for the pivotal role he played in ushering peace in Assam. Along with his expertise in COIN, he has been a key player in transforming Assam Police into a citizen-centric, service-delivery force. His work in developing and implementing rehabilitation programs for victims of violence has been universally appreciated, including by UNICEF. He is also a national award-winning filmmaker and an accomplished writer. Apart from holding office as the General Secretary, he will also be looking at Geopolitical Affairs.

Lead for Global Affairs, Governing Body: Shri Harsh Vardhan Shringla, IFS (Retd) was the Chief Coordinator for India’s G20 Presidency, former Foreign Secretary of India, former Indian Ambassador to Thailand & the USA and High Commissioner to Bangladesh. He was critical in promoting India’s Neighbourhood First and Look East policies. He was a key pillar in the success of India’s G20 Presidency where he took the G20 to India’s hinterlands, including NEI. He has carved a niche for himself in developing strategic alliances, thereby, putting India firmly on the global map and shall lead Global Affairs within the organisation.

Lead for Trade & Connectivity: Shri Nazeeb Arif, Executive VP & Head of Corp. Communications, ITC Limited, leads the Trade & Connectivity vertical. With nearly four decades of experience in business and industry, he has promoted sub-regional economic co-operation that puts NEI at its core. He is a recipient of the prestigious United States Asia Environmental Partnership – Environmental Leadership Award. Before joining ITC, he was the Secretary General & CEO of the Indian Chamber of Commerce. He is known to be a champion of sustainable development in the business world.

Lead, Area Studies: Dr. Samudra Gupta Kashyap, Historian & Chancellor, Nagaland University, heads the vertical of Area Studies. A widely acclaimed scholar and journalist, Dr. Kashyap has to his credit four decades of reporting NEI to the outside world. Author of several books primarily focused on NEI and S/SEA, he is acknowledged to have ushered in systemic changes in Nagaland University. A distinguished alumnus of Indian Institute of Mass Communication, New Delhi, he holds a PhD Degree in Management.

Treasurer and Lead, Critical & Emerging Technology: Shri Subimal Bhattacharjee, Tech Policy Adviser and Columnist, leads the vertical of Critical & Emerging Technology. Shri Bhattacharjee is a well-known policy adviser on technology and security issues. He has been a member of the advisory committee of Global Commission on Internet Governance. He has also served as a policy expert on two UN led programs on the subject of critical and emerging technology. He is a regular contributor to several print and TV media organisations in India, on all matters pertaining to technology. Previously, he was the Country Head of General Dynamics, India. He also presides as the treasurer of the organisation, financial planning, budgets and ensures financial accountability.

Lead, Culture Studies: Smti. Sunita Bhuyan, violinist & HR Professional, leads the vertical of Culture Studies. A renowned violinist, she regularly performs around the globe. She is also the Chief Mentor of Atos Prayas Foundation, a visiting faculty of IIM Shillong on Music and Aesthetics & CEDEP France and is also a consulting practitioner for various prestigious forums and organisations. She was awarded by Pope Francis at the Vatican City for her work on music therapy with underprivileged children, cancer patients and people with disability.

Lead, Research & Admin: This will be headed by Shri Abhijan Das. Shri Das has been involved in national security affairs for over a decade, counterterrorism being one of his key focuses. He also has a decade of consulting experience working with Fortune 100 companies. He has completed his M.Sc. in Strategic Studies from S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore with specialisation in Terrorism Studies. He looks at research initiatives, managing project teams and resources as well as general administration.

SHARE

Society to Harmonise Aspirations for Responsible Engagement

Website: www.theshare.in
Email: office@theshare.in