[**Deadly symbiosis**](https://www.dawn.com/news/1757186/deadly-symbiosis)

[Mohammad Ali Babakhel](https://www.dawn.com/authors/2112/mohammad-ali-babakhel) Published June 1, 2023

TERRORISM is theatre, and the internet a stage where terrorists can perform certain roles. For example, while executing a terrorist attack, planners also want to use it to attract an audience, inspire new talent, multiply a feeling of insecurity and erode public confidence in the state. The internet provides a ready platform to further these goals. As a cheap and easy means of spreading propaganda, the internet offers interactive opportunities for violent non-state actors (VNSAs) to connect with their supporters and amplify their voice. For secure communication, the dark web offers anonymity. Anonymous identities and end-to-end encryption are added attractions that increase the challenge for law enforcement agencies.

The internet provides instant, worldwide, multilingual access at low cost. In our part of the world, extremist propaganda is now disseminated in English, Bangla, Hindi, Tamil, Gujarati, Urdu and other vernacular languages through social media. Dabiq, an online magazine published by the militant Islamic State in different langua­ges, opts for purpose-driven communication. Dabiq employs professional communication to educate, persuade, and col­l­a­b­o­rate with global audiences. In its recruitment calls, the magazine includes theological and legal content authored by clerics and intended for professional audiences like doctors, lawyers, and engineers. Similarly, a cyber-warfare magazine for jihadists titled Kybernetiq provides information to the militants about technology and enables them to participate in the cyber war against their enemies. Through such magazines, militant groups also educate their readers on how to protect their anonymity.

The IS considers technology a crucial instrument in waging war. For secure communication and propaganda, different enc­r­y­ption apps, including Tashfeer al-Jawwal, Asrar al-Ghurabaa, and Amn al-Mujahid, were developed and distributed by the group among its followers. Encryp­ted communication enables militants to talk without LEAs listening in. IS is also known for its credible offensive cyber capability, which means it has the capacity to steal sensitive data. Reportedly, the group lures hackers with hefty financial packages.

Because of the significant presence of youth in cyberspace, terrorist groups have made it a norm to record video messages prior to suicide attacks. These messages glorify the volunteerism of the bombers and are aimed at attracting new recruits. Separately, handlers also identify those who share pro-militant and anti-West posts on social media. Those considered potential sympathisers are contacted by authorised persons who engage them in radical conversations. After assessing their mindset, they share videos and other material with them. If the targets express interest, they are enrolled for different tasks in terrorist outfits.

Technology is a crucial instrument of war for extremists.

The internet is proving to be a gold mine for extremists: a repository for self-training, a breeding ground for self-radicalisation, and helpful in obtaining information related to potential targets. The internet has also reduced the need for physical tra­ining facilities. Furthermore, it provides precious information that enables many to gain knowledge without physically attending any training facility. Open-source information also allows militants to collect data and conduct passive reconnaissance.

Point 5 of the National Action Plan (NAP I) listed strict action against literature, newspapers, and magazines promoting hatred, extremism, sectarianism and intolerance, while point 11 banned the glorification of terrorists and terrorist organisations on print and electronic media. Point 14 included measures against the abuse of the internet and social media for terrorism. While point 2 of NAP II combined the gist of these three points in NAP I, it desires action against the spread of terrorism through media (electronic, print, and social media), communication, and cyber networks.

Implementation of these points requires the allocation of more funds, capacity building, improved policing capabilities within cyberspace, public education and outreach. Identifying, eliminating, and combating anonymous, nameless, and faceless elements within cyberspace will impr­o­ve the peace index, public safety, and nati­o­nal security — but the real irritant is our intense romance with traditional approa­ches. Defeating VNSAs is not possible without understanding their evolving narrative, communication strategy and techniques, as well as the linkages between socio-economic dynamics and ethno-political marginalisation amplified by mass media and social media. Pakistan needs to improve its monitoring and analytical cap­a­bilities with respect to cyberspace. Inves­tments in cyber policing will pay significant dividends. The state needs to listen to experts in this area and modify its counter-narrative and strategy accordingly.

*The writer is author of Pakistan: In Between Extremism and Peace.*

[**Twitter: @alibabakhel**](https://twitter.com/alibabakhel)

*Published in Dawn, June 1st, 2023*