

## Countering terrorism through the Net

By Elina Noor

**PREVENTION THROUGH EDUCATION THE BEST CURE:** *Censoring or taking down terrorist sites will only drive extremists further under the surface*

RADICAL and extremist websites used to be fairly rudimentary – low on graphics and heavy on text.

For groups ranging from Stormfront to the Liberation Tigers of Tamil Eelam, the early days of the Internet offered a quick and easy platform to establish presence, disseminate information, and invite benefaction from a global audience.

Communication in the 1990s usually flowed on passively, from web administrator to reader. More forward-thinking groups, however, encouraged interaction through online bulletin boards or discussion forums, generating a constant exchange of views and ideas and significantly, sustaining interest in the cause.

Those were the days of dial-up when the transfer of large parcels of data transfer would have taken hours. These days, with broadband, there are daily rueful ruminations of life in the front lines of Iraq and Syria, accompanied by smartphone photos and videos, as well as rallying sound bites to arms in 140 characters or less. In an age of running news feeds, a barrage of status updates, and 100 hours of YouTube videos uploaded every minute, the battle for mindshare and attention is fierce.

It is no longer enough to simply capture and retain interest but to shock and awe the already overloaded senses in increasingly visceral ways for maximum impact. This explains in part the savvy social media outreach of affiliates of the self-proclaimed Islamic State and their calculated visual releases of bombings and beheadings in multiple languages. Reception to this social media onslaught has been disturbingly encouraging, if the number of online followers and tens of thousands of foreign fighters believed to be in Syria are to be believed.

The instinctive reaction is to block, filter, censor, or take down extremist sites and uploads because of their sheer number and reach. Barring exceptions, however, there are at least three reasons why the alternative of leaving them online may be more useful.

**FIRST**, they offer a trove of information and insight into planned attacks, the individuals and psychology behind them, as well as methods and means of operation. This is especially so when access to closed groups is gained undercover, offering valuable intelligence for law enforcement purposes.

**SECOND**, shutting down sites will only result in the launch of other sites under different domain names or worse, force communication underground. Only four per cent of the World Wide Web as we know it is indexed by search engines, which means the millions of networked pages that we access constitutes just the surface of the Internet. The other 96 per cent is hidden in the Deep Web, where content is stored in its own specialised database and cannot be found through the usual search engines. As has happened before, censoring or taking down sites at the tip of the Internet iceberg will simply drive extremists further under the surface, masked by greater anonymity.

**THIRD**, leaving sites online allows for counter-narratives to respond to the sales pitch of extremists and address their shortcomings. The idea is to avail and encourage alternative messaging in a marketplace of ideas so that when impressionable individuals search for answers, they are offered options. Done right and supported by credible authorities, counter-narrative should at the very least, provoke a rethink of the superficial.



This last point, especially, demands a capacity for critical thinking – the ability to question veracity, to compel cogency of argument, and to consider if not accept different viewpoints. Sure, there are occasions when filtering or taking down uploads or sites may be warranted but these are tactical counter-measures that will at best, temporarily fix and at worst, aggravate the systemic problems which are often rooted in the physical world.

Self-radicalisation does not take place in a vacuum nor does it take place solely online. To respond to only this facet is to ignore the fact that there is a whole ecosystem both online and offline that drives an unassuming individual to radicalism, a radical to extremism, and an extremist to terrorism. Counter-terrorism requires a dynamic, multi-pronged and multi-stakeholder approach that adapts to the technology and the times as nimbly as terrorists themselves do. But while we adjust and respond to the supply side of Terror.com, perhaps we should begin with old school basics as a long-term approach to preventing the demand side of the equation: by guiding our children to question and to reason so that what their online searches bring up can be processed and rationalised in their own super computers – the brain – instead of being taken at face value.

***Elina Noor is ISIS Malaysia Assistant Director, Foreign Policy and Security Studies***