INSTITUTE OF STRATEGIC STUDIES

web: www.issi.org.pk
phone: +92-920-4423, 24
fax: +92-920-4658

Issue Brief

(Views expressed in the brief are those of the author, and do not represent those of ISSI)

Countering Terrorism Online

July 18, 2017

Written by: Sarah Akram, Research Fellow *Edited by: Malik Qasim Mustafa*

Terrorism has gone from an unrelenting yet trivial security concern to one of the most important security problems of our times. There are few countries that do not suffer from some form of terrorism. Though many cyber attempts at terrorism fail, some groups end up being successful in their endeavors to recruit, disseminate and spread their ideology. In this regard, the United Nations (UN) has welcomed major partnership initiatives with tech giants to counter terrorism online, which includes tech giants like Facebook, Microsoft, Twitter and YouTube. Although these four companies have already created removal policies against terrorists, but joint initiatives with the UN can have a greater impact.

The *Global Internet Forum to Counter Terrorism* partnership launched by the UN will help further strengthen these 'counter-speech' protections through research - evidence-based efforts and technical and policy decisions around the removal of terrorist content, as specified by the UN Executive Directorate.[1] The growing presence of modern terrorism on the Internet is at the nexus of two key trends: the democratisation of communications driven by user-generated content on the Internet; and the growing consciousness of modern terrorists of the potential of the Internet for their purposes.

During the recent decades, the world has witnessed the surfacing and proliferation of cyber terrorism. Modern terrorists have become exposed to new opportunities for exerting mass psychological impacts as a result of technological advances in communications. The network of computer-mediated communication is ideal for terrorists-as-communicators: it is decentralised, it cannot be subjected to control or restriction, it is not censored, and it allows access to anyone who wants it. Websites are only one of the Internet's services used by modern terrorism; there are many other facilities in the Net — e-mail, chat rooms, e-groups, forums, virtual message boards, YouTube and Google Earth — that are used more and more by terrorists. The great virtues of the Internet — ease of access, lack of regulation, vast potential audiences, fast flow of information and so forth — have been converted into the advantage of groups committed to terrorising societies to achieve their goals. Similarly, psychological warfare, online

[1] "UN welcomes major partnership initiative with tech giants to counter terrorism online," http://www.un.org/sustainabledevelopment/blog/2017/06/un-welcomes-major-partnership-initiative-with-tech-giants-to-counter-terrorism-online/

indoctrination, recruitment and mobilisation, planning and coordination as well as disinformation are also put to perfect use by the terrorists.[2]

However, due to the growing dependence of terrorists on the Internet, the essential war between terrorists and counterterrorism forces and agencies is certainly a critical one and in order to counter and foil the intended destruction by the terrorist groups, governments must take effective steps to counter the use of online forums to counter terrorism. Collaboration with tech giants as well as the UN can help in limiting and destroying the plans of terrorist groups. As Pakistan struggles to get rid of terrorism, cyber/online terrorism also figures on its agenda. The National Action Plan (NAP), which was formulated soon after the Army Public School (APS) Attack in December, 2014 also included a point, which called for the formation of a committee to counter online terrorism. Apart from this, the Pakistan Telecommunication Authority (PTA) has also taken many initiatives to block and intercept illegal dissemination of information on the internet. PTA has been taking action against pages on social media and online videos posted by terrorist groups.

The challenges for the states regarding cyber terrorism are serious because security of both the government and civilians is at stake. The terrorists can make best use of the cyber technology in fulfilling their aims and goals. The problem is in the execution of laws of cyber crime as technology is advancing very rapidly. However, Pakistan must enforce cyber laws strictly and take steps towards bilateral and multilateral cooperation in this regard as this is a completely new front on which the threat of terrorism is to be fought, as online terrorism also adds to the vulnerability of the public at large.

[2] Gabriel Weimann and Katharina Von Knop, "Applying the Notion of Noise to Countering Online Terrorism," http://www.tandfonline.com/doi/pdf/10.1080/10576100802342601?needAccess=true