**Policing the dark web**

Khawaja Khalid Farooq

Tuesday, Mar 28, 2023

The internet has revolutionized the world in many ways. It has made communication faster and more efficient, and it has given people access to information on a scale that was previously unimaginable. However, the internet also has a dark side: known as the dark web.

The dark web is a part of the internet that is not accessible through regular search engines like Google. It is mostly used by criminals, including terrorists, to communicate and conduct illegal activities. A whole Pandora’s box of problems has arisen due to the relationship between terrorism and the dark web, including how terrorists use the dark web. Currently, there are more challenges in combating terrorism on the dark web than there are possible solutions.

The dark web provides a level of anonymity and privacy that is not available on the regular internet. This makes it an attractive platform for terrorists who want to communicate, recruit new members and plan attacks. Terrorist groups also use the dark web to raise funds and spread propaganda.

One of the most well-known terrorist groups that use the dark web is ISIS. In 2015, ISIS created a propaganda magazine called Dabiq, which was published in multiple languages and distributed on the dark web. The group also used the dark web to recruit new members and to communicate with them securely. ISIS operatives also used the dark web to raise funds by selling merchandise such as T-shirts and flags, and by accepting donations in cryptocurrency.

Another example of a terrorist group that uses the dark web is Al-Qaeda. The group has been using the dark web since the early 2000s to communicate with its members and to distribute propaganda. Al-Qaeda also used the dark web to raise funds through Bitcoin donations.

The dark web presents many challenges in combating terrorism. The first challenge is the anonymity provided to terrorists who can use pseudonyms and encrypted communication to hide their identity and location. This makes it difficult for law-enforcement agencies to track down and arrest terrorists.

Then there is the sheer size of the dark web which is estimated to be 500 times larger than the regular internet and is constantly growing. This makes it difficult for law-enforcement agencies to monitor all of the websites on the dark web.

The use of cryptocurrency by terrorists has complicated the issue of terrorist financing to new heights. Cryptocurrency, such as Bitcoin, is a digital currency that can be used to make anonymous transactions. Terrorists use cryptocurrency to raise funds and to transfer money without detection.

Law-enforcement agencies around the world are using technology to investigate terrorism on the dark web. One technology that is commonly used is artificial intelligence (AI). AI algorithms can be trained to detect patterns of communication and behaviour that are consistent with terrorist activity. For example, AI can be used to analyze online conversations to identify individuals who are discussing terrorist activities.

Another technology used in the investigation of terrorism on the dark web is machine learning. Machine learning algorithms can be used to analyze large volumes of data to identify patterns and anomalies that may be indicative of terrorist activity. Machine learning algorithms can also be used to track the movement of cryptocurrency to identify terrorist-financing networks.

Law-enforcement agencies are also using Big Data analytics to investigate terrorism on the dark web. Big Data analytics can be used to analyze massive amounts of data from various sources to identify patterns of behaviour that are consistent with terrorist activity. Big Data analytics can also be used to monitor social media and other online platforms to identify individuals who may be involved in terrorist activity.

All this is easier said than done, though. Even highly resourced police forces struggle with the sheer volume of data on the dark web, which raises questions regarding Pakistani LEAs who barely know about this phenomenon.

Preventing terrorism on the dark web requires a multi-pronged approach. Law-enforcement agencies must work closely with technology companies to identify and shut down websites and platforms that are being used for terrorist activity. They must also work with financial institutions to identify and freeze the funds of terrorist organizations. This cooperative effort is currently missing in our law-enforcement culture, which needs to be inculcated if we are to be ready for the future.

There are several possible solutions to combat terrorism on the dark web. The first solution is to increase the capabilities of law-enforcement agencies to monitor the dark web. This could involve increasing funding for cybercrime units and investing in new technologies that can track down terrorists on the dark web. However, even in developed police forces with tremendous resources, this is difficult. How would our LEAs cope in this scenario? They have to if they want to stay relevant in the coming times.

Another way is by increasing cooperation between law-enforcement agencies across different countries. Terrorist groups operate across borders, and it is important for law-enforcement agencies to work together to combat them. This could involve sharing intelligence, coordinating investigations, and extraditing terrorists to face trial in their home countries.

It is important to increase public awareness of the dangers of the dark web. Many people are unaware of the existence of the dark web and the risks associated with it. By increasing public awareness, people can be more vigilant and report suspicious activity to law-enforcement agencies.

The writer is a retired inspector general of police and ex-head of Pakistan’s National Counter Terrorism Authority. He tweets @Kkf50