TERROR IN THE DARK

HOW TERRORISTS USE ENCRYPTION, THE DARKNET, AND CRYPTOCURRENCIES

Nikita Malik

Terror in the Dark explores how terrorists and extremists use the Darknet. It highlights the following trends:

- **TERRORISTS USING ENCRYPTION TO HIDE:** Jihadist recruiters use the Darknet to plan and launch terrorist attacks because detection by law enforcement is less likely. While initial contact can be made on surface web platforms, further instruction is often given on end-to-end encryption apps such as Telegram.
- **TERRORISTS USING CRYPTOCURRENCY TO EVADE DETECTION AND FUNDRAISE:** By fundraising and facilitating transactions online with bitcoin, terrorists and other criminals can avoid interference from financial regulators who would prevent their operations.
- **TERRORISTS USING THE DARKNET FOR RECRUITMENT PURPOSES:** Given the largely inaccessible nature of encrypted channels like Telegram and areas of the Darknet, mass recruitment rarely takes place on these channels. Instead, groups like Islamic State draw interested sympathisers from the surface web and social media into the Darknet for further interaction and indoctrination.
- **TERRORISTS USING THE DARKNET AS A RESERVOIR OF PROPAGANDA:** Artificial intelligence programs do 'bulk' removals of extremist content on social media platforms, but much of this material resurfaces on the Darknet.

The following recommendations focus on fostering human intelligence and capacity building in this area:

Technology companies should create a self-regulatory system to audit extremist content, and make this information publicly available.

The British government should create an Internet Regulatory Body.

More resources should be dedicated to the Joint Terrorism Analysis Centre (JTAC) to build intelligence capital on the Darknet.

Social media companies should work with law enforcement to ensure that extremist material is archived to understand patterns of behaviour.

CRT
Centre for the Response to Radicalisation and Terrorism

THE HENRY JACKSON SOCIETY

TERROR IN THE DARK

HOW TERRORISTS USE ENCRYPTION, THE DARKNET, AND CRYPTOCURRENCIES

Nikita Malik

Case Study techniques used to identify Darknet users

Pen or Trap Orders:

- Gathers data on communications to and from an IP address, without revealing the contents of the communications.
- Trap and trace shows what numbers (or IP addresses) have contacted the IP address being monitored. A pen register shows outgoing communications.
- *Case Study: SR1.*

Bitcoin Exchange Companies:

- Can provide governments with user records.
- *Case Study: Blake Benthall (SR2).*

Infiltration of 'staff areas' of Cryptomarketplaces:

- Software data of the administrator can be viewed by FBI or other intelligence agents. This is then matched with records gathered from the Bitcoin exchange company.
- *Case Study: Blake Benthall (SR2).*

Sting:

- This technique targets customers, not vendors. The buyer is apprehended upon receipt of the illicit package.
- *Case Study: Liverpool ricin case.*

Network Investigative Technique (NIT):

- Requires seizure of server of site.
- Also known as Computer Network Exploitation, and involves the use of malware to proactively hack a site.
- *Case Study: Playpen.*

Criminal Error:

- Extensive search of the internet and user's 'digital history' to uncover details which lead to identification, e.g. email address (in the case of both *SR1* and *SR2*). Once email address is known, IP address can be found.
- This was also significant in the *Playpen* case – configuration errors by the site's creator led to the discovery of the true IP address of Playpen's server.

Source: compilation of information in report

CRT
Centre for the Response to Radicalisation and Terrorism

THE HENRY JACKSON SOCIETY