‘Big picture’ platforms boost fight against online terror activity

In recent years, online terrorism-related content has grown in 'velocity, volume and variety'. Paris Image credit - Flickr/Takver CC BY SA 2.0

The fight against terrorism-related content and illegal financing online is speeding up thanks to new platforms that join up different internet-scouring technologies to create a comprehensive picture of terrorist activity.

The idea is that when an online tool discovers a fragment of information it can be added to a constellation of millions of others - revealing links that might otherwise have gone undetected or taken much longer to uncover.

In 2017 legislation, the EU said that serious crimes, such as attacks on a person’s life, or the threat to commit them, can qualify as a terrorist offence if they have the goal of intimidating a population or destroying a country’s economic, political or social structures.

Terror groups ranging from the Islamic State to right-wing supremacist organisations use digital media to disseminate propaganda, recruit and train people, raise funds and move money around, and communicate with each other.

In recent years, such content has grown in 'velocity, volume and variety' according to Professor Babak Akhgar, director of the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research at Sheffield Hallam University, UK.

Appearing in multiple languages and media forms, this content penetrates not just the easily accessible surface web but also the deep web - accessible to an ordinary person but not to a search bot, for example, password-protected sites - and the deliberately anonymised and concealed dark web, which can only be accessed by using special software.

With the rise in this material online, law enforcement agencies are looking for ways to trawl through it more efficiently, says Jonathan Middleton, acting head of international programmes at the Police Service of Northern Ireland (PSNI).

According to him, agencies currently tend to use different tools in isolation, and therefore may miss the connections between pieces of information. 'They might use one tool to do a web search, for example, and another to monitor online social media,' he said.

Researchers with a project called DANTE are now combining various tools into a single platform, to automate the tracking of money flows, and dig out propaganda and training materials.

Fundraising

Online fundraising for terrorism has shifted in recent years onto the dark web, where cryptocurrencies such as Bitcoin, Ethereum and others are harnessed to channel money made from, for example, trade in firearms and illegal drugs.

> 'It's about trying to make it more efficient and effective for the analyst.'
>
> *Jonathan Middleton, Acting Head of International Programmes, Police Service of Northern Ireland*

Ernesto La Mattina, head of the Homeland Security Unit at the Italian software company Engineering Ingegneria Informatica, and project coordinator for DANTE, says that while cryptocurrencies are renowned for being secure, each chain of transactions has to be initiated by someone and that provides a point of vulnerability, such as an email address, where identity can be probed. Linking this snippet with information extracted from other arenas can help law enforcers 'reconstruct the entire crime storytelling,' he said.

DANTE is integrating tools such as stylometric analysis in which algorithms note distinctive aspects of a text attributable to a specific person such as the frequency of use of certain words, grammatical structures and sentence patterns. This provides insights into the educational level, gender or age of the writer. In lab tests using known participants, its accuracy is around 90%, says La Mattina.

The platform also includes tools that analyse audio – translating, transcribing and trying to identify the speaker – and videos. The video tools use algorithms to alert analysts to interesting objects or features such as weapons, tattoos or flags.

The five languages chosen for the project – English, Arabic, Italian, Portuguese and Spanish – are analysed in two ways. A deep semantic analysis of the original text is carried out as well as an analysis of its English translation.

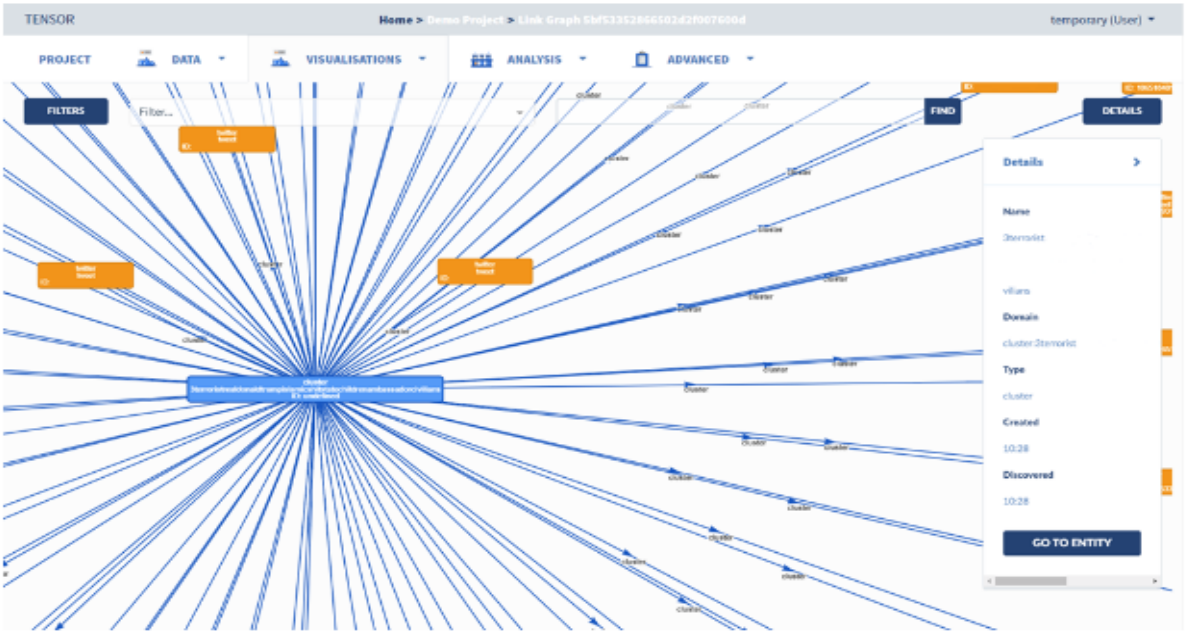
Both DANTE and another pan-European project, TENSOR, work with national law enforcement agencies which stipulate what they need in their operations. TENSOR is in fact coordinated by a law enforcement agency, PSNI, and focuses on detecting the planning of terrorist events, radicalisation and recruitment. Counterparts in Belgium, Germany, Greece, Spain and the UK are piloting the project.

As with DANTE, TENSOR researchers are pulling together myriad types of analysis onto the same platform so the relationships between pieces of information can be collated and considered on a single computer screen. Tools include semantic analysis of the relationships between words, artificial intelligence, deep learning, social media analytics, multi-media forensic analysis and classification.

Tampered

A multi-media forensic tool might, for example, assess a propaganda video to see whether it has been tampered with – for example, by splicing in a scene that comes from a movie, says Prof. Akhgar, a TENSOR collaborator.

Classification tools arrange millions of data fragments in a graspable set of hierarchies, or taxonomies. They can be arranged like an exploding star packed with content that reveals itself in ever-increasing detail at a click.



The TENSOR platform uses tools like link graphs to join up different pieces of information. Image credit - International Programmes Office

'It's about trying to make it more efficient and effective for the analyst, who will ultimately have to review any data that's retrieved or identified and make that recommendation on what action should be taken,' said Middleton, project coordinator for TENSOR.

Last month, at the first prototype testing of the TENSOR platform, Middleton says law enforcers were excited about the amount and kind of information that can be returned.

'They're seeing all those individual pieces of information in one program, in one desktop,' he said. 'So rather than scrolling between different software solutions and trying to extract information out of each solution they are actually getting all the analytics back in a much more useable manner.'

All this has to be achieved while respecting privacy and legal protection, which is a great challenge, say the projects' collaborators.

'There are lots of tools providers out there who are doing all sorts of things,' said Prof. Akhgar. 'But as soon as they would bring that piece of kit to the operational environment they would find that it's not legal to use it, or the data obtained from it is not admissible in court, or they are breaching the General Data Protection Regulation, or breaching human rights law or whatever it is within the EU framework of legislation. And the tool becomes useless.'

He said: 'It is critical that everything which we pull together is done on the basis of fundamental rights and GDPR guidelines.'

The research in this article was funded by the EU. If you liked this article, please consider sharing it on social media.