SPOTTING THE PATTERN

Dr Brenton Cooper *reveals why OSINT technology is a primary weapon against resurgent extremism online*

It could hardly be starker. The boss of MI5 said the UK faces the most complex threat environment ever. The country is subject to the malign activities of the Russian state, murder plots from Iran, a resurgence of lethal threats from Islamic extremists such as al-Qaeda and its affiliates and from far-right activists.

In his speech at the Counter Terrorism Operations Centre in London, Ken McCallum also said he was surprised by the increasing number of children investigated for terrorism, many of them radicalised online. In fact, said McCallum, one-in-eight people investigated is under-18. He was clear that it is hard to overestimate the influence of online platforms in inspiring and informing potential terrorists – especially the young.

The question is how to counter this sea of poisonous content, with much of it designed to attract the young, isolated and angry. The enormous volume of data involved across the globe's online platforms is now far beyond the analysis capabilities of any team of analysts. The time has come for more canny adoption of open-source intelligence technology that uses ethical AI for advanced, accurate and automated analysis on a vast scale right across all the dark recesses of the internet.

AI-enabled open-source intelligence technology is essential because everyone in society now spends so much time online, leaving digital footprints which can include risk indicators that are essential to intelligence investigations. UK government's Prevent programme estimates adults spend up to quarter of their time awake online, with 18-24-year-olds averaging more than five hours.

One-in-eight people investigated for terrorism are under the age of 18

The high-profile case of Shamima Begum and her two friends is a good example of how online radicalisation affects young people. They were teenage girls when they slipped out of the UK in 2015 to join Islamic State, having been radicalised by the extremist terror group's online content.

Youth is a significant factor in most online radicalisations. In the half-century between 1950 and 2000 there were 85 mass casualty events, most of them perpetrated by adult men. In the two decades following the advent of the internet in 2000 the number of events was more than double those in the previous 50 years and on one estimate, six of the nine most deadly attacks were committed by men aged 21 or younger.

In the US, for example Payton Gendron was 18 when he murdered ten black people in Buffalo, New York in 2022, and was sentenced to life imprisonment without parole. He is a self-confessed white supremacist who in his manifesto, released on 4chan, stated he was radicalised by the internet. He also referred to his use of the social platform Discord, which is popular with gamers. He was also able to find radicalising content on more mainstream channels like YouTube and Reddit. Not only did Gendron document his plans online he also cited the inspiration he took from other mass-killers such as Brenton Tarrant in New Zealand. Both live-streamed their crimes.

Tarrant had published his own manifesto, which has proved to be influential through social media. People attracted to far-right extremism include John Earnest, who attacked a synagogue in Poway, California, in April 2019, and Patrick Crusius, who attacked an El Paso Walmart in August 2019. Both shooters posted manifestos on 8chan before their attacks.

Use of the internet prior to mass shootings is obviously not limited to white supremacists. The 2019 Pensacola Naval Air Station shooter was a Saudi national who posted his hatred of the US and its people online prior to his attack that killed three people.

A 2022 study for the UK Ministry of Justice added to the body of evidence about the radicalising power of social media. It found most of Britain's convicted terrorists had been turned into extremists very largely by what they read and saw on the internet. Many became followers of Islamic State, but others were violent animal rights campaigners. Half of those radicalised online had some form of mental health disorder, the study found. It also revealed the proportion radicalised wholly or in-part online had risen from 43 percent in 2013-15, to 85 percent in 2016-18.

The radicalisers are expert at luring in the frustrated, vulnerable and lonely, building a spuriously personal connection while offering entry to an exclusive group of the dedicated. The sharing and amplification of conspiracy theories is a standard technique.

Senior UK and US police officers warned earlier this year, however, that many drawn to extremism are attracted by violence rather than ideology. In a BBC interview, Rebecca Weiner, Deputy Commissioner of Intelligence and Counterterrorism at the New York Police Department described online extremism as an: "everything, everywhere, all-at-once threat environment".

Matt Jukes, the UK's Head of Counter-terrorism Policing said young people were watching extreme "dehumanising content" online with gaming one of the gateways to this dark world. The conflicts in Gaza and Lebanon have only served to intensify Islamic or antisemitic extremism.

The internet has become the most potent factor disseminating extremism. Even the most graphic video content can be a recruitment tool, while anonymity permits the posting of disinformation that appeals to the emotions of the susceptible or promotes conspiracy theories and false accounts of real events.

The channels and platforms extremists use are always changing and, alongside the massively popular mainstream social media platforms, include 4chan, 8chan/8kun, Discord, Telegram, Tik Tok, WeChat and Weibo. The "chan" sites harbour niche far-right communities, permit the posting of extreme content and provide anonymity for users – "anons" – who are identified only by letters and numbers.

DIGITAL FOOTPRINTS CAN INCLUDE RISK INDICATORS VITAL TO INTELLIGENCE INVESTIGATIONS

Speed, ease of access and anonymity are key factors, but the scale and reach of the internet are also what has made online radicalisation so effective. The time, effort and finances extremists need for global propaganda have been drastically reduced.

Almost all this data is available for intelligence and law enforcement agencies to analyse, but the sheer scale and the complexity of collecting, filtering and analysing it to detect risks for intelligence purposes is beyond human capabilities. Across social media and other online platforms, OSINT (Open Source Intelligence) investigators and their small teams have gigabytes of data to trawl through. Without technology the task is impossible even for the most well-resourced intelligence teams.

The effective exploitation of OSINT demands AI, machine learning and allied analytical technologies such as natural language processing deployed within ethical guidelines that enhances and does not replace the decision making of skilled intelligence analysts. Alongside human intelligence tracking the activity of known activists and the people they are in contact with, it is possible to study patterns of behaviour online to learn from past successes and mistakes.

OSINT and social media intelligence (SOCMINT) capabilities identify suspicious patterns of behaviour, levels of engagement and probable goals for content such as disinformation posts.

With far-right extremists there is a strong tendency to network and to cite each other, leaving a trail of content through online conversations, posts and comments. Established groups often want to recruit while Islamic terror organisations know they can inspire lone operators. This inevitably leads them into more public online spaces where they are more exposed to investigation.

Combined with other forms of human and traditional signal intelligence, OSINT technology can provide vital

insights from these sources that would never otherwise be attainable. It goes beyond keywords to assist in analysing images, videos, memes and obviously, posts and other forms of textual content.

Advanced OSINT algorithms keep up with the changes in meaning that online jargon and memes undergo as groups adopt them. It can detect text in images through optical character recognition technology.

RADICALISERS ARE EXPERT AT LURING IN THOSE WHO ARE FRUSTRATED, VULNERABLE AND LONELY

By using advanced data collection combined with AI-enabled risk analysis, advanced OSINT technology can automate complex intelligence tasks, helping analysts sift through vast amounts of data and identify relevant information in a matter of seconds. This is particularly useful when dealing with far-right groups, which have large online presences generating a significant amount of content.

The technology enables intelligence agencies and policing organisations to build a picture of motivations and methods. Once identified, relationships and networks can be understood along with activity on other forums, platforms or social media accounts and the Dark Web.

Sentiment and emotion analysis are part of the insights now achievable. Employing multi-lingual data capabilities, OSINT and social media intelligence (SOCMINT) technology are also capable of working effectively on foreign-owned platforms.

The most advanced AI-enabled risk analytics can detect threats in images, videos, written text, or digital network connections. This technology can save analyst teams hours and days of manual data manipulation with ongoing, repeatable and automated collection alongside assessment of diverse data mediums.

The reach of OSINT technology extends far across billions of social media accounts, a huge range of forums, platforms and official information sources, and the Dark Web. Smart prioritisation cuts out the noise while augmented intelligence enhances human decision-making and improves the processing of data.

A holistic approach to OSINT is important so intelligence teams are not left juggling between different and often incompatible technologies. An OSINT platform that is able to dovetail with workflows and operate intuitively can vastly augment the expertise of experienced intelligence and security professionals.

Users can fine-tune the AI models to detect novel risks quickly without depending on access to specialised data science expertise. Sentiment analysis, rapid filtering and detection of key words and phrases, along with built-in obfuscation provide anonymity.

With intelligence and counter-terrorism chiefs highlighting the dangers of online radicalisation at a time when public finances are stretched, the case for adoption of advanced, AI-powered OSINT technology has never been stronger.

Democracies are up against highly skilled, social media-savvy extremists who are constantly pushing out their violent ideologies online across the full range of social media. Their ability to innovate, subvert remains as well-developed as ever, as they seek to inspire, recruit, sow mayhem and mistrust.

We are never going to live in a world where there are enough intelligence analysts with the right skills to manually examine the huge volumes of data on global social media platforms. Yet this is primary resource that, if analysed properly, enables the authorities to stay several steps ahead of the threat actors and implement effective prevention strategies. The case for OSINT technology has never been stronger than it is now ●

Dr Brenton Cooper is CEO & Co-founder of Fivecast.

Prevent estimates adults spend up to quarter of their time awake online, with 18-24-year-olds averaging more than five hours

Picture credit: gloucester2gaza