DETECTING EXTREMIST PLOTS ONLINE

Dr Brenton Cooper *explains why policing needs AI-driven open-source technology*

The foiling of an extremist bomb plot targeting the huge audience at a Lady Gaga concert in Brazil shows the value of open-source intelligence.The anti-LGBTQ extremists sought to radicalise teenagers online through digital cells, inspiring them to use improvised explosives in the attack against the estimated two-million audience. Brazilian authorities gained advance warning of the plot, which gave them time to intervene and arrest two people, preventing any potentially lethal casualties from occurring.

Approximately 2.5-million people attended the free concert held on Copacabana Beach

Picture credit: Buda Mendes/Getty Images

Reports say the extremists, used violent and self-harm-related content to build an online community of teenagers, employing coded language and extremist symbols. This use of violent, graphic content that attracts young people to extremist causes is a trend that threatens to overwhelm police authorities and intelligence organisations.

The problem for the authorities is dealing with the volume of material posted online, usually under pseudonyms and often on obscure platforms. Statista estimates 5.42-billion people will use social media this year, generating a huge volume of data.

Problems are amplified by a lack of moderation on many platforms and algorithms that help spread content, leaving authorities to determine whether those posting malicious material are part of a wider group and what their aims are.

Intelligence teams must also keep up with the changes in platforms that extremists use, which include 4chan, 8chan/8kun, Discord, Telegram, TikTok, WeChat and Weibo. The 'chan' sites are often home to the far-right, providing anonymity for users to share radical beliefs.

The task of analysing this information from fast-emerging groups with little formal structure is substantial and often beyond the resources of policing or counter-terrorism analysts. The volume and velocity of online data growth is too great for human capabilities. Many policing organisations only have embryonic open-source intelligence (OSINT) capabilities and therefore cannot afford to employ an army of fully trained open-source data analysts.

To filter and analyse this mass of data at scale and speed, organisations must adopt more advanced technology. Automation saves analysts days of manual data analysis. AI-powered, OSINT tools are purpose built for detection of extremist content and can use analytics to establish connections between individuals and groups. Without requiring expertise in data science or data-management, intelligence teams can configure AI-enabled risk detectors to uncover content relevant to their investigations across publicly and commercially available information. The technology will map online entities and establish links between threat groups and extremist ideologies, creating a new set of vital capabilities.

Combined with other forms of human and traditional classified intelligence, OSINT technology provides vital insights that teams wouldn't be able to extract themselves. It goes beyond keywords to assist in analysing images, videos, memes, posts and other forms of multimedia content. Advances in OSINT algorithms enable solutions to keep up with the changes in the meaning of online jargon or symbols as threat groups adopt them. If the technology cannot reveal the main entity behind content, associates with online links can often be identified through the power of analytics.

Policing intelligence teams can store video from multiple accounts, reviewing material as required – a critical advantage when groups may post content and then quickly take it down in a bid to thwart detection.

Well-honed capabilities highlight not only content, but also suspicious patterns of behaviour, establishing levels of engagement and probable goals. Such insights would never otherwise be attainable. Platforms using OSINT algorithms detect text in images through optical character recognition technology and can deploy sentiment and emotion analysis and smart prioritisation cuts out noise, allowing augmented intelligence to enhance human decision-making. This means that no time is wasted once human intelligence officers believe the evidence suggests a high likelihood of a plot.

Once investigators are on the trail of a plot or believe online extremists are actively seeking to recruit, OSINT technology can expand the search across many diverse online data sources, including the Dark Web, marketplaces, people databases, watch lists and curated datasets of known threat groups.

As the frequency of new threats grows and more young people are at risk of exposure to extreme content, policing organisations need advanced open-source social media intelligence technology to supercharge their own intelligence skills and experience. Benefiting from automation and highly sophisticated algorithms, AI-driven open-source intelligence platforms are set to play a vital role in protecting our youth and communities at large from the scourge of online extremism ●

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