NETWORK OF EXCELLENCE FOR RESEARCH
IN VIOLENT ONLINE POLITICAL EXTREMISM

CASE STUDY

FUTURE TRENDS: LIVE-STREAMING TERRORIST ATTACKS?

Maura Conway & Joseph Dillon
Dublin City University

Email info@voxpol.eu
www.voxpol.eu

Introduction

Magnanville, 13 June, 2016, around 8pm: policeman, Jean-Baptiste Salvaing has been stabbed to death outside his home. Forcing his way into the house, the attacker murders Jessica Schneider, who also worked for the police, by cutting her throat. The couple's three year-old son is taken hostage by the killer, Larossi Abballa. Prior to a three hour stand-off with police negotiators, Aballa turns to social media to broadcast and justify his actions, dedicating them to his 'Emir' Abu Bakr Al-Baghdadi (Hume et al 2016). It is the first time a terrorist has used a live-streaming service in the midst of an attack. It is unlikely to be the last.

Live video footage of violent events is not in itself new. Live footage from 1972's Black September attack on the Munich Olympics was disseminated globally via the television crews already gathered at the scene to cover the games. In 2001, live television footage of the second plane hitting the World Trade Center astounded many and supplied real-time confirmation that a terrorist attack was taking place.

Camera-enabled mobile telephones were in their infancy in 2001, with their widespread take-up not happening until 2003 – 2004. Over time, a plethora of social media platforms sprung up based, wholly or in part, on widespread use of mobile telephones' still image and video capture technologies. These include Flickr (2004), YouTube (2005), Instagram (2010), and Snapchat (2011). Mobile phones with high specification cameras and mobile data access are now ubiquitous and, together with live-streaming services such as Twitter's Periscope (2015) and Facebook Live (2015), have facilitated a significant recent uptake in live-streaming of a wide variety of events and activities. The potential impacts of this were foreshadowed by Mark Lukasiewicz, then Vice President for Digital Media at NBC News, after shaky footage leaked of Saddam Hussein's 30 December, 2006 execution, when he remarked that "[i]t brought to a fore the sense that, wow, this is a ubiquitous technology…Cameras are now in places where cameras never used to be. That's transformational" (Bauder 2007).

Technological adaptability is key to the survival of any terrorist organisation. Given that live-streaming is rapidly catching on within the general population, it is inevitable that there will be further intersection of these two phenomena. Ultimately, a terrorist group or lone actor will attempt to live video stream a terrorist attack.

Video specialist, Alex Zambelli, writing in *The Guardian* in 2013, identified a "significant quality gap" between television broadcasts and the then best available streaming technology that, he said, was likely to last for some time. For our purposes however, David's 2010 observation that "if the camera phone image we take has an impact on the future, it will be not because of its quality, but because of its content" is more relevant. Rather than issues of video quality, what is most important as regards live video streaming, as opposed to film or television streaming, is the proliferation of video-ready Internet-connected mobile telephones and users with the wherewithal to use them when they find themselves at 'the right place, at the right time' or, in the case of violent extremist and terrorist attacks, 'the wrong place, at the wrong time.'

Live reporting news crews may number a few thousand at any given time, but "participatory journalists," as Bowman and Wills (2003) might label them, or "citizen

journalists" as they have become more generally known, will soon be counted in the hundreds of millions. Periscope's 'parent's' user base exceeds 300 million people and Facebook is now approaching two billion users. With the popularity of live-streaming set to surge in the coming months and years, the number of people at any given event—large or small, public or private, formal or informal, planned or *ad hoc*, celebration or crisis, peaceful or violent—ready to live broadcast will be countless.

In the past terrorist groups had to manipulate the world's media for propaganda purposes. Granted, a handful of terrorist groups established their own television outlets; Hizbollah's al-Manar Television is the most well-known of these. But terrorist groups with the necessary financial and other resources to establish their own professional media operation have always been in a small minority. The Munich Olympics were targeted by Palestinian terrorists at least partly because of the enormous media presence already in place. As the attack began to play out, this mammoth collective media spotlight was effortlessly refocused from the sporting event, so that around 900 million people in at least one hundred different countries saw portions of the hostage-taking and the ensuing counterterrorism operation unfold live on their television screens (Hoffman 2006, 69). When the North World Trade Center tower was struck by American Airlines Flight 11 in September 2001, a nearby film crew happened to capture the event. Undoubtedly, the planners of the 9/11 attacks were cognisant of the inability of the media to look away from something shocking or terrifying, and thus the high likelihood of the second attack being recorded. The footage of the second tower being struck and the subsequent collapses will remain one of the most watched live TV events in history.

Today, it is unthinkable that such a shocking event in such a highly populated area would not be covered from a huge number of angles by large numbers of users live-streaming on various online platforms. In fact, within hours of Periscope being released for iPhone it was used by over a dozen bystanders to live-stream video of a building fire in Brooklyn, caused by a gas explosion (Popper 2015).

Bystander Accounts and Recordings

Web 2.0 or the social web is heavily reliant on user generated content (i.e. blogs, social media posts, podcasts, videos, images, etc., created by third-party users). A specific type of user generated content is described and discussed below: content generated by bystanders to terrorism-related events, largely terrorist attacks, which has become increasingly commonplace. One upshot of this is that contemporary terrorists need no longer concern themselves with directly ensuring mass media coverage of the type described above. Social media has made journalists, and even newsmakers, of the average user.

One of the earliest and probably still one of the most well-known incidents of a bystander social media role in a terrorism-related incident, took place in 2011 when Sohaib Athar, an IT consultant on a break from work, informed his Twitter followers of strange events in Abbotabad, Pakistan more than an hour before President Obama informed the rest of the World (Bowman et al 2014). Athar, known as @ReallyVirtual on Twitter, started commenting on unusual helicopter activity in the area at about 1am on 2 May. He continued to tweet as a "windows shaking bang" shortly followed. Over the

next few hours he gathered rumours and compiled observations about an event "that would soon have the world riveted" (Bell 2011). The raid was "shrouded in every bit of secrecy the US government could muster," but it was completely unanticipated that a simple bystander could break the news of a top-secret military operation (Amble 2012). Realising the significance of the event mid-stream Sohaib tweeted "Uh oh, now I'm the guy who live-blogged the Osama raid without knowing it" (Olson 2011).[1]

In London in 2013, Michael Adebolajo sought out the onlookers' cameras and, hands soaked with Lee Rigby's blood, calmly justified what he and his accomplice, Michael Adebowale, had just done. There were no satellite trucks or television crews, only a handful of bystanders. An ITV news editor rushed the amateur cameraperson to the broadcaster's headquarters 12 miles away and the Blackberry footage of the murderer's speech was replayed by worldwide media just hours later (Halliday 2013). Neither the speech nor the act itself was broadcast in real-time, but the event was live Tweeted by an aspiring London rapper 'Boya Dee'. He began tweeting moments after the attack began and continued until the pair of murderers were shot by police (Nelson 2013).

The Paris attacks of November 2015 were covered by hundreds of people on social media. The final notes of the Eagles of Death Metal concert being interrupted by gunfire were captured on Instagram (Kayali and O'Rourke-Potocki 2015). Andrew Smith, a British academic, tweeted unfolding events at the Bataclan Theatre from his nearby apartment (Paget 2015). Benjamin Cazenoves, injured and hiding on the first floor of the Bataclan, used Facebook to urge the police to raid the building as quickly as possible—a post shared over 22,000 times. Periscope was in such use during the attacks that it crashed for nearly an hour at around 6:30pm that evening (Rodriguez 2015).

In a testament to the increasing popularity of live-streaming, in 2016 a number of violent extremist and terrorist attacks across Europe and the United States were captured and relayed live by bystanders. The March 2016 Brussels Airport and Metro station bombings were live-blogged by several social media users. Luke Mac an Bháird, a 22 year old Irish student, arrived at Brussels international airport minutes before the attacks began and live-tweeted the panic that ensued as people realised an attack was ongoing (Lynch 2016). The sniper killings of five police officers (and their immediate aftermath) in Dallas on 7 July 2016 were extensively covered by Periscope and Facebook Live users. One Facebook Live user, Michael Kevin Bautista, was at ground level, across the street from the main gun battle waged between police and Micah Johnson, the sniper. His footage, taken from behind a tree, captures a chaotic volley of gunfire as he attempts to narrate the scene (Mezzofiore 2016).

The opening shots outside of a McDonalds of the 22 July, 2016 Munich shootings were also filmed, and later broadcast by the world's media. One man who had a view from his apartment of the closing stages of the attack live-streamed it to his Facebook page. In the footage, the murderer can be seen on the rooftop of the shopping centre below the

[1] In a strange twist on the role Twitter played in events, five years later the CIA retroactively live-tweeted Operation Neptune Spear. In what was regarded as a self-congratulatory public relations exercise by many Twitter users, @CIA tweeted step-by-step, the intelligence gathering process (making sure to justify the role of torture in the affair), the progress of the commandos who entered the building (resplendent with maps and diagrams), and ultimately the killing of Bin Laden and the disposal of his body at sea, 1,500 kilometres away.

apartment as police surround the area and civilians are evacuated, some in ambulances (Tiefenthaler 2016). Islamic State (IS)-affiliated Telegram accounts immediately began to spread the videos and laud the attacker, but it later transpired that the shooter, 18 year-old Ali David Sonboly, a German-Iranian, was inspired by extreme right ideology. The attack, which left nine people dead, was so widely covered by bystanders on their mobile phones that the police established an online portal where such videos could be submitted to aid the investigation (Ewing 2016).

Terrorists' Live Reporting of Attacks

Violent jihadi organisations, including al-Qaeda, but particularly IS, have a fairly lengthy history of live video recordings of, amongst other events, suicide attacks and beheadings of captives. Live-blogging of attacks is a much newer departure.

Al-Shabaab broke the mould in 2013 with their Twitter strategy during the Westgate shopping mall attack in Nairobi, Kenya. The Westgate attack saw Al-Shabaab dispense with a reliance on bystanders and news crews to report their actions, which they instead live-tweeted themselves. Around midday on Saturday, 21 September, four Al-Shabaab militants opened fire on shoppers and restaurant-goers outside Westgate before making their way inside from two different entrances. When the dust finally settled, the tally of wounded was over 200 and 67 people were dead. Twitter played a core role in events. People used it to discern and publicise information about what was going on whilst, at the same time, authorities used it to urge people to be careful about what was being posted online and frequently asked users to remove content that was considered operationally compromising. Crucially though, throughout the attack al-Shabaab used Twitter to supply its own account of events and to explain and justify its actions (Gollum 2013).

It is important to note that terrorists are not wholly innovating when they employ media in this way. Much has been made about terrorist groups social media know-how, Menkhaus (2014) asks if al- Shabaab's use of Twitter and similar activity by other groups is in fact as 'savvy' as so many have claimed, or simply demonstrates "basic competence in its use of video, Internet, Twitter and a thesaurus that millions of tech-proficient teenagers worldwide can match." Neither al-Shabaab nor IS nor any other terrorist group employs the world's leading social media innovators, they have simply replicated what any brand-conscious entity would do.

Responses to Terrorists' Use of Live-streaming

The available responses to terrorists potential use of live video streaming are worth considering now, despite the absence to-date of a live-streamed attack. Why? Because in order to be effective, solutions will already need to be in place if or when footage from an ongoing attack is live-streamed by the perpetrators.

After the murders in Magnanville, Facebook announced that it would expand its team responsible for reviewing live content. However, with a growing user base of nearly a quarter of the world's population, it is doubtful even Facebook has the budget to employ enough people to manually review all video content as it goes live. They have been testing the review of live-streams as they go viral however, and before they are reported

by mainstream media, with reportedly some success. Again the problem of quantity remains; relatively shortly, the number of highly trending streams will simply be too much to be reviewed manually. Facebook is also experimenting with artificial intelligence tools that can "interpret and categorise live videos in real time," but the company has no plans to apply such tools on a large-scale as of yet (Chaykowski 2016).

There has been considerable progress in other areas though. An experimental model for automatically monitoring and flagging violent or terrorist acts caught on live CCTV was "completely and successfully implemented" by Chandana (2011). Similarly Vinel *et al* (2014) detail how improved broadband connections will enable live-streaming of CCTV footage to vehicular networks, allowing for more rapid responses to crime and terrorism. Transposing this work into the online sphere should not be a herculean task. Up until very recently, computers were not good at identifying even simple objects in images. The main driver behind to improve this situation comes from the marketing and advertising sector; it would be a huge boon if a company could use an algorithm to identify specific products in users' social media images to focus even more highly targeted advertising in their direction.

The consensus among the developer community is that steady progress is being made:

> "From programs that help the visually impaired and safety features in cars that detect large animals to auto-organizing untagged photo collections and extracting business insights from socially shared pictures, the benefits of image recognition, or computer vision, are only just beginning to make their way into the world — but they're doing so with increasing frequency and depth" (Weiner: 2016).

Piggybacking on market-driven successes might be a better option than trying to generate bespoke solutions in the context of terrorism.

Recently, some of the major video hosting platforms have quietly started to move towards automated systems to remove extremist material. Using unique digital fingerprints called 'hashes' Internet companies can easily remove content with matching 'fingerprints.' The problem, in terms of live-streaming, is that this method cannot automatically block photos or videos that have never been seen before (i.e. that are not in the 'fingerprint' database) (Menn and Volz 2016). Menn and Volz say Internet companies are considering ways to block extremist content before it can spread, but have nothing to gain from being open about their censorship methods. If extremists and terrorists learn about content blocking procedures they might figure out ways to circumvent them—wrapping a Kalashnikov in a blanket, for example, would be enough to confuse an algorithm.

Without doubt a plethora of false positives will be identified by any automated detection methods. The average innocent live-streamer would be understandably upset when an innocuous video of theirs is incorrectly flagged as extremist content and removed. The key for tech companies is to automate as much as possible, and limit the content that requires manual review. Questions of freedom of speech, censorship, etc. will continue to plague the Internet community, caught between the conflicting demands of politicians, law enforcement, and their users. False positive incidents should dramatically reduce as the software continues to 'learn' such that automated flagging of potential extremism and terrorism content should become more effective over time.

Counterargument(s) and Conclusion

In conclusion, a counterargument may be that live video streaming is not entirely attractive to violent political extremists and terrorists. IS, for example, has been very successful at producing edited live video recordings whilst al-Shabaab found live micro-blogging suited their needs.

Live video streaming may be particularly unattractive to those who wish to carefully edit and shape their narrative. IS is reportedly able to ensure their victims are calm prior to videoed executions by practising mock executions numerous times so their hostages are not aware they're actually about to be murdered (Ratcliffe 2015). Larossi Abballa's Facebook live-stream was circulated as a video recording post-attack, but edited to remove any mention of the three-year old hostage before being disseminated by IS propaganda outlets. This desire to edit and control the narrative will not always be possible when it comes to live video streaming. It's possible that during live-streaming, unintended outcomes that were not choreographed play out, perhaps shedding light upon the perpetrators' clumsiness, and potentially resulting in ridicule.

The ongoing attempt to retake Mosul is a watershed moment for live-streaming. Most major news channels and many independent news outlets used one of the currently popular live-streaming applications to follow events. In this media fray, IS were conspicuous for their absence. IS are known for using GoPro cameras and even drones to film their battlefield prowess, an unwillingness to stream their exploits live should probably not surprise us however. In March 2016 an IS fighter captured his own death using a GoPro camera. One month later a video detailing the chaos and disorganisation of IS fighters in battle surfaced (Withnall 2016). IS, or any terrorist group, are potentially loathe to take the risk of live-streaming such events should they go against them. There is also a risk for perpetrators in conflict zones that potential gathering of valuable location data from live-streamed footage by intelligence analysts could backfire dramatically. On the other hand, perpetrators of marauding attacks within the EU may not have the same concerns regarding the risk of, for example, an instant drone attack.

IS will probably continue to be early adopters of some social media capabilities and affordances and discard others. They are therefore likely to engage to some extent with live-streaming in the near future. They will without doubt however, carefully consider the counterarguments. Upon reflection and following, perhaps, some unintended consequences, editing recorded content and posting as soon as possible thereafter, will probably remain their preference to retain editorial control. The online activities of IS-inspired or 'remote controlled' lone actors are more difficult to determine however and bear watching.

References

Amble, J.C. 2012. 'Combating Terrorism in the New Media Environment.' *Studies in Conflict & Terrorism* 35(5): 339-353.

Bauder, D. 2007. 'Cell-Phone Videos Transforming TV News.' *The Washington Post* 7 January: https://goo.gl/DV7QV1.

Bell, M. 2011. 'Sohaib Athar's Tweets from the Attack on Osama bin Laden: Read Them All Below.' *The Washington Post* 2 May: https://goo.gl/ifTDqP.

Bowman, S. and Willis, C. 2003. 'We Media: How Audiences are Shaping the Future of News and Information.' *The Media Centre* July: https://goo.gl/kfHYvp.

Bowman, N., Lewis, R.J. and Tamborini, R. 2014. 'The Morality of May 2, 2011: A Content Analysis of US Headlines Regarding the Death of Osama bin Laden.' *Mass Communication and Society* 17(5): 639-664.

Chandana, S. 2011. 'Real Time Video Surveillance System Using Motion Detection.' *Institute of Electrical and Electronics Engineers*, Conference Report 26 January: https://goo.gl/zANMzs.

Chaykowski, K. 2016. 'Terrorism Suspect's Use of "Facebook Live" Stream Highlights Challenges of Live Video.' *Forbes* 15 June: https://goo.gl/SCy5lm.

David, G. 2010. 'Camera Phone Images, Videos and Live-streaming: A Contemporary Visual Trend.' *Visual Studies* 25(1): 89-98.

Ewing, J. 2016. 'Munich Police Ask Witnesses for Video of Attack.' *New York Times* 22 July: https://goo.gl/Mxx3To.

Gollum, M. 2013. 'Kenya Attack: Why al-Shabaab Live-tweeted the Assault.' *CBC News* 24 September: https://goo.gl/nTl64E.

Halliday, J. 2013. 'Woolwich Attack First UK Murder to be Transmitted 'Live' on Internet.' *The Guardian* 19 December: https://goo.gl/Y8f7MB.

Hoffman, B. 2006. *Inside Terrorism* (New York: Columbia University Press).

Hume, T., Isaac, L. and Cruikshank P. 2016. 'French Terror Attacker Threatened Euro 2016 in Facebook Video, Source Says.' *CNN* 14 June 14: https://goo.gl/EmxJmC.

Kayali, L. and O'Rourke-Potocki, H. 2015. 'The Paris Attacks, as Told Through Social Media.' *Politico* 15 November: https://goo.gl/T2UJc9.

Khetan, A. 2009. '60 Dark Hours at Hotel Taj.' In H. Baweja (Ed.), *26/11 Mumbai Attacked* (New Delhi: Roli Books): 46-83.

Lynch, S. 2016. 'Brussels Attacks: Belgian Police Hunt for Suspect.' *The Irish Times* 23 March: https://goo.gl/fK0qea.

Menkhaus, K. 2014. 'Al-Shabaab and Social Media: A Double-Edged Sword.' *Brown Journal of World Affairs* 20(2):309-330.

Menn, J. and Volz, D. 2016. 'Exclusive: Google, Facebook Quietly Move Toward Automatic Blocking of Extremist Videos.' *Reuters* 25 June: https://goo.gl/NnmGVh.

Mezzofiore, G. 2016. 'Man Streams Attack on Dallas Police on Facebook Live.' *MashableUK* 8 July 8: https://goo.gl/ZjQ7rH.

Nacos, B. 2010. *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post 9/11 World*, Third ed. (Boston: Longman).

Nelson, S.C. 2013. 'Woolwich Attack: Rapper Boya Dee "Offered £75k For Story" After Tweets Go Viral.' *The Huffington Post* 23 May: https://goo.gl/ZWp4O7.

Oh, O., Agrawal, M. and Rao, H.R. 2010. 'Information Control and Terrorism: Tracking the Mumbai Terrorist Attack through Twitter.' *Information Systems Frontiers* 13(33): 33-43.

Olson, P. 2011. 'Man Inadvertently Live Tweets Osama Bin Laden Raid.' *Forbes* 2 May: https://goo.gl/00Bilw.
Paget, A. 2015. 'Liverpool Lecturer Live Tweets Paris Shootings.' *Liverpool Echo* 14 November: https://goo.gl/ck7w6u.
Popper, B. (2015) 'There Was an Explosion in New York City, and Seconds Later I Was Watching it Live on Periscope.' *The Verge* 26 March: https://goo.gl/fqSCbI.
Ratcliffe, R. 2015. 'ISIS Tricked Victims into Appearing Calm with Beheading Rehearsals.' *The Guardian* 10 March: https://goo.gl/Qx9S4s.
Rodriguez, S. 2015. 'Twitter's Periscope Crashes Under Heavy Traffic Due To Paris Attacks.' *International Business Times* 13 November: https://goo.gl/KifEji.
Shuster, S. 2016. 'Munich Police Face Questions Over False Tweets During Shooting.' *Time* 25 July: https://goo.gl/Vt9DYi.
Skipper, B. 2015. 'Call of Duty: Activision Live-tweets Fake Terrorist Attack to Market Black Ops 3.' *International Business Times* 30 September: https://goo.gl/OIOYWl.
Tiefenthaler, A. 2016. 'Streaming the Munich Shooting Live.' *The International* 23 July: https://goo.gl/VXe33z.
Weiner, K. 2016. 'Why Image Recognition is About to Transform Business.' *TechCrunch* 30 April: https://goo.gl/pwUoCU.
Withnall, A. (2016) 'Dead ISIS Fighter's Headcam Video Shows Chaos and Disorganisation on Frontline.' *Independent* 27 April: https://goo.gl/QNcITC.
Zambelli, A. 2013. 'A History of Media Streaming and the Future of Connected TV.' *The Guardian* 1 March: https://goo.gl/zIxI5f.