Radicalisation Awareness Network
RAN

Webpage: ec.europa.eu/ran

twitter | facebook | linkedin | youtube

28/10/2019

EX POST PAPER

RAN C&N – Communications After an Attack, 1-2 October 2019, Lisbon, Portugal

Communications After an Attack

As part of preventing and countering violent extremism (P/CVE), where we seek to limit the strategic effectiveness of terrorists and other extremists, we also need to understand the communications environment after an attack, and know how to communicate effectively in this context. Even more so than the rest of the P/CVE domain, this is a multi-stakeholder challenge. We must consider the role of local, national and supranational governments, civil society organisations, traditional and non-traditional media, the police and strategic communications practitioners. Thus, this paper aims to consider this topic from a range of perspectives, bridge the gaps between them, share best practices, and assemble some guidance for the wider Radicalisation Awareness Network (RAN) on how to communicate effectively. This paper considers the strategic dynamics of media and communications in the post-attack context, good practices and lessons learned from several high-profile terrorist attacks, and the roles of different stakeholders, in order to establish some recommendations and solutions for the sector.

Product of the RAN Centre of Excellence
Authored by **Jonathan Russell**
RAN Centre of Excellence.

Communications After an Attack

The problem we're tackling

"Terrorism is theatre: terrorists want a lot of people watching, not a lot of people dead." ([1])

By this, terrorism theorist and academic Brian Jenkins means that terrorist organisations don't purely seek to tactically use violence to commit murder; they do so strategically for ideological motives, to instil fear in a population or to achieve political change. To achieve this, they require societies to watch the terrorist attack, and for the incident to dominate the news agenda in the hours and days thereafter. Terrorists fully understand human behaviour and the media environment in this regard, and know that the more spectacular, the more symbolic and the greater the death count, then the greater the overreaction from governments, and the greater the strategic effect among populations. In this regard, terrorists know how to communicate after an attack. Likewise, it should be acknowledged that other extremists (not the perpetrators of the attack itself) will seek to leverage an attack to further their own objectives, and this is an important aspect of the topic.

A wide range of stakeholders who share a common goal of preventing or countering violent extremism are likely to communicate after an attack: the police, journalists, municipalities, practitioners, the general public, and others. However, we should recognise that they have different communications objectives and therefore different messages, messengers, media and calls to action when communicating.

The strategic effect of communications after an attack

As part of P/CVE, where we seek to limit the strategic effectiveness of terrorists and other extremists, we also need to understand the communications environment after an attack, and know how to communicate effectively in this context.

Previously, such as with the 9/11 attacks in the USA or the 3/11 attacks in Madrid, al-Qaeda aimed to achieve political change. In 2001, al-Qaeda aimed to draw the West into a War on Terror, and get the USA to commit troops to unwinnable conflicts in Afghanistan and Iraq in which they would be overstretched, exhausted and abrasive towards local populations vulnerable to radicalisation. In 2004, just before the Spanish elections, al-Qaeda aimed to affect voters' opinions so that they would vote for a party that would withdraw Spain's commitment to the Iraq War.

In recent years, Daesh pivoted to a different strategy, where they aimed to radicalise Western populations, in order to increase a foreign fighter phenomenon and build the sustainability of their desired caliphate in Iraq and Syria. They aimed to empower radicalised Westerners through giving them the motivation and tools to commit attacks in the West; they aimed to stoke a clash-of-civilisations psychology, whereby non-Muslim populations would equate all Muslims with terrorism and even radicalise them reciprocally towards far-right extremism; and

([1]) Jenkins, B. M. (1974). *International terrorism: A new kind of warfare*. Santa Monica, CA: The Rand Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/papers/2008/P5261.pdf

they sought to provoke Western governments to move away from their liberal and democratic ways and bring in draconian laws, which would eventually have the same effect ([2]).

Case Study – Malign Influence Post-Attack

The 2017 Westminster attack gives one of the most rounded examples of the complex communications environment after an attack. Fifty people were injured and six people died when jihadist terrorist Khalid Masood drove his car into pedestrians on Westminster Bridge and subsequently stabbed PC Keith Palmer on the grounds of the Palace of Westminster. We now know his radicalisation journey, which included conversion to Islam, time in prison, an education in Saudi Arabia and his obsession with Western foreign policy in the Middle East. However, the 72 hours of communications both immediately before and in the days after this attack are even more interesting if you consider who attempts to benefit:

- **Before his attack, he used WhatsApp to send his contacts a manifesto setting out his commitment to jihadist ideology and his grievances with Western foreign policy. He wanted to gain strategic effect from his acts, regardless of their effectiveness.**
- **Within 24 hours, Daesh made a claim that he was a soldier of the caliphate. However, there has been no proven link between them. Daesh wanted to gain strategic effect from his acts, regardless of their command and control.**
- **Within 2 hours, far-right extremist Tommy Robinson travelled to Westminster and live-streamed his analysis, using his usual rhetoric to blame Islam the religion rather than politicised ideology Islamism, or the actions of one man. He too wanted to derive strategic effect from the terrorist act, despite it being perpetrated in the name of the opposing ideology.**
- **Within 24 hours, an out-of-context photo of a female passerby in a hijab went viral online, with the accompanying narrative that Muslims turn a blind eye to terrorism and are in some way complicit. It has subsequently been proven that Russian state-owned media and a coordinated Russian troll farm helped this image to achieve vitality, and that it was in fact part of a disinformation campaign. They too saw an opportunity to gain strategic effect from this incident 3 000 km away.**

In many ways, this attack serves as a comprehensive case study for this topic to help practitioners understand the 360-degree communications environment before they consider planning their response. However, it must be noted that the communications environment is in constant flux. For example, perpetrators of more recent incidents, such as the Christchurch terrorist attack in 2019, have live-streamed their attack to thousands of followers ([3]).

We can look back to other recent terrorist incidents and see a pattern of behaviour among states, societies and media afterwards. We see states trying to reassert control and trust in

([2]) Russell, J. (2016). *Le Monde's leadership against Daesh propaganda of the deed*. The Global Coalition against Daesh. Retrieved from https://theglobalcoalition.org/en/le-mondes-leadership-against-daesh-propaganda-of-the-deed/
([3]) Facebook. (2019). *Combating hate and extremism*. Retrieved from https://newsroom.fb.com/news/2019/09/combating-hate-and-extremism/

their security policies, aiming to reduce fear among their populations. We see fear and anger among societies. And in the media, we often see a blame game, we see sensationalist reporting, and we see them trying to piece together the story from incomplete information. What about on social media? We see all of these different reactions come together, and perhaps change over the hours and days after a terrorist incident. One notable dynamic on social media after a jihadist terrorist attack is an immediate spike in Islamophobia.

Indeed, both the mainstream media and social media companies have been criticised in recent years for the way that terrorists have exploited their channels to be more effective communicators. Even back in the early 2000s, Al Jazeera was criticised for the way in which it ran al-Qaeda's statements claiming attacks, with many claiming that they must have interaction with terrorists or support their objectives and ideologies. More recently, there has been a debate about how news websites have amplified Daesh propaganda by hosting their videos ([4]). Jihadists and far-right extremists are well known for embracing technology and social media, and social media companies have long been considering how to effectively police their platforms to prevent terrorist use of the internet.

Case Study – Other Influence Post-Attack

Aside from the aforementioned sources of malign influence, other stakeholders also communicated after the incident, and the target audiences of the above communicators would likely also be exposed to the following:

- **British broadcaster Channel 4 covered the incident like all media. However, in their haste to be first, at one point they erroneously claimed that the perpetrator was infamous al-Muhajiroun supporter Abu Izzadeen. It was later shown that Izzadeen was in prison and therefore not the perpetrator. This shows the difficulty of reporting with incomplete information, and how the pressures of the situation can result in inadvertent misinformation.**
- **A range of official voices also communicated: the Prime Minister and the Leader of the Opposition delivered their condolences to victims, thanked the emergency services, and attempted to build national unity. In the same vein, the London Mayor and several interfaith leaders led a candlelit vigil.**
- **The Head of the Metropolitan Police gave clear information about the incident and the subsequent investigation, attempting to reassure Londoners. They communicated with a press release and on their social media channels. There was an early signal about the motivation of the attacker, when it was announced that the Counter-Terrorism Command was leading the investigation.**
- **The Home Secretary appeared on television to call for government backdoor access to encrypted messaging services, reinforcing government policy in an area in which they had not previously managed to make progress, and aiming to blame social media companies for failure to prevent the attack.**

([4]) Marthoz, J. P. (2017). *Terrorism and the media: A handbook for journalists*. Paris, France: UNESCO. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000247074

In addition to this, civil society organisations in P/CVE had (and have) a role to communicate post-attack. Many are invited to comment in traditional print and broadcast media. These and others communicate on their own social media channels. Some will work in partnership with governments; others will pursue their own priorities. The same complexities that apply to the communications environment therefore also apply to civil society groups; thus, the recommendations below should be adapted for all stakeholders.

Communicating effectively post-incident

No two terrorist attacks are identical. However, there are some similarities in the response required. This includes acting under enormous time pressure, having to make do with imperfect resources, having a clear decision-making and strategic approach in the face of incomplete information, and emotions running high.

Just having knowledge and understanding set out in the problem statement above, knowing what questions to ask, and being aware of the different contextual dynamics are already beneficial to communications practitioners. However, preparation and skills development are crucial in order to be able to communicate effectively ([5]). The general recommendations made below are structured into two main sections: **planning and collaboration**; and **communication**. Where relevant, we pull out specific recommendations for different sectors.

PLAN AND COLLABORATE

- If you have strategic communication in place without crisis communications, then the plan is not good. Even if the plan is a very simple narrative and some draft language that can be appraised in the moment of crisis, that is better than having nothing. Stakeholders in local government may have more control over their communications, and a greater audience, than they are used to having. This may lead to resource issues and unexpected hurdles such as website bandwidth. These sorts of things could be included in the crisis communications plan. **All stakeholders in the P/CVE sector should proactively consider this hypothetical situation and establish a plan ahead of time, and a communications strategy as part of this. For communications practitioners such as those running a counter-narrative campaign, you might also like to think about the appropriate things to communicate in this scenario.** If the objective of your communication strategy is not clear, then your message is very likely not going to be effective. **Refer to the GAMMMA+ section below for further guidance and the helpful resource from SAFE-COMMS ([6]).**

- Pre-established vertical relationships to ensure multi-level, informed responses, making sure the right voices are included, and the effective creation of an action plan with clear lines of communication are essential to success. You don't make friends in a crisis. Key partnerships need to be made in advance. **Consider which partnerships will be important (e.g. police, local institutions, local communities but also media outlets) and build these ahead of time: trusted relationships can rarely be built during crisis. Talk**

([5]) Reed, A., & Ingram, H. J. (2019). *Towards a framework for post-terrorist incident communications strategies*. The Hague, the Netherlands: International Centre for Counter-Terrorism. Retrieved from https://icct.nl/publication/towards-a-framework-for-post-terrorist-incident-communications-strategies/

([6]) Shpiro, S., Díaz Fernández, A. M., Hargie, O., Nikolov Madzharov, S., Möhrle, H., & Nomikos, J. (2011). *SAFE-COMMS Terrorism crisis communication manual for public authorities*. Retrieved from https://faculty.biu.ac.il/~sshpiro/pdf/SAFE%20COMMS%20Manual%20final_en_0605.pdf

about the potential crisis scenario to ensure you are all on the same page. Cities that recover the fastest recover best, and the best route to recovery is through multi-stakeholder partnerships.

- Provide space for **local civil society** who can be effective messengers. Their expertise and credibility can help in countering propaganda and creating alternative narratives.
- Consider the relationship between terrorism and communications, the effects and the importance of giving meaning to attacks. Think about the media perspective too, who may face difficulties in deciding on what and how to report on terrorist attacks. Journalists should consider why it matters and how their reporting can influence society. They could minimise the negative communications effect of terrorism through balanced and truthful reporting, providing context and **positive stories**, and build relationships with other stakeholders. Similarly, social media firms are also thinking about this: current and future partnerships between governments and tech companies can help to stop extremist content (spread by the perpetrator for example, like in the Christchurch attack) going viral.

Case Study – Communications After an Attack

Following the jihadist terrorist attack on Manchester Arena, local government were thrust into a communications response scenario. They had previously planned and tested a crisis communications plan, so were able to activate this to great effect immediately after the incident. It was easy to stand up to this plan and would have been more difficult without the relationships with the police and the mayor. This enabled them to have a coherent communications strategy across all sectors, with a single narrative and similar language to share and use, meaning they could repeat key messages and have a touchstone to turn back to.

Their mantra was that *cities that recover fastest, recover best*. And that drove their communications strategy, and they opted to respond with love rather than hate. While there was a spike in hate crime and Islamophobia after the attack, they mitigated this with positive alternative narratives. They decided not to use potentially divisive politicians' voices; instead, they featured faith leaders, community leaders, representatives from emergency services, and also the opportunity for the city to show civic leadership and reinforce a message of love during vigils and through the events in the immediate aftermath. The Council however, along with other authorities continued to appropriate civic leadership messages. Audiences were receptive to this, and focused on these images and messages of solidarity. Indeed, many of the independent campaigns and response activities established post-attack continued this narrative. These activities were from the ground up and authentic from communities, which the Council amplified rather than coordinated.

They found it easy to work with local media but that responding to national and international media, in the context of an attack on a concert held by a global American superstar, was more difficult. Indeed, their crisis communications approach was challenged by the behaviour of some media: for example, the day after the vigil, they woke up to loads of broadcast trucks parked outside their office and the New York Times shared pictures of the detonation device and what happened in the foyer. They used social media to great effect to share messages, but were overwhelmed by the messages, and found that they received a friendlier response on Twitter than Facebook. They received such a lot

of traffic to their website, which became a trusted news source, that it crashed. Their book of condolences played a key role as it helped people to share their grief.

- Have a **dedicated communications team** ready in case of a crisis (including backup) and ensure that they **receive the necessary support and aftercare**.

- For the media, it is important to **be fair and balanced** when reporting, which might be facilitated by having a specific journalist for P/CVE-related topics. If you are not sure what happened, **be factual, reassuring, empathetic** and don't interpret. It is advisable to **shut down the comment section** when reporting on a terrorist attack, as the worst reactions are often found there. Journalists reporting on terrorist attacks should ensure they **have a verified account**, to avoid a takedown by the social media platforms. They should be careful not to spread extremist content — for example, journalists need not use videos or images of terrorist propaganda, or post links to a manifesto, as that will likely be detected as extremist content and taken down online, and is also inadvertently helping terrorists.

- Likewise, governments should also consider their role and the value of a multi-stakeholder approach. They tend to work in silos; however, **open lines of communication with media and civil society organisations is important after an attack, including to spread a cohesive whole-of-government narrative** to general populations and vulnerable communities alike.

COMMUNICATE

- **Be aware that you are not the only one communicating**; sources of malign influence also use the aftermath of an attack to try and gain recognition and polarise society. Understand the communications approaches of other positive stakeholders too, so that you can play a positive role within the broader ecosystem.

- Timing is really important. Governments experience a tension between being the **first** to communicate, in order to restore stability and reassure their citizens, being **transparent** and calming in order to achieve these effects, and being **informed**, so as not to inadvertently spread misinformation. Other stakeholders should also think about these three pillars of responding to an incident.

- It is perfectly acceptable to actively decide not to communicate. For example, you may decide after an incident that you will wait until you have more information about the motive of the perpetrator, before communicating. However, you should likewise remember that inaction can also have a communications impact. For example, this decision not to communicate until you have more information may leave a vacuum in which stakeholders with less noble intentions communicate to your target audience and negatively impact your objectives. **Even if you don't know for sure what happened, it is a good idea to let people know that you are working on it.**

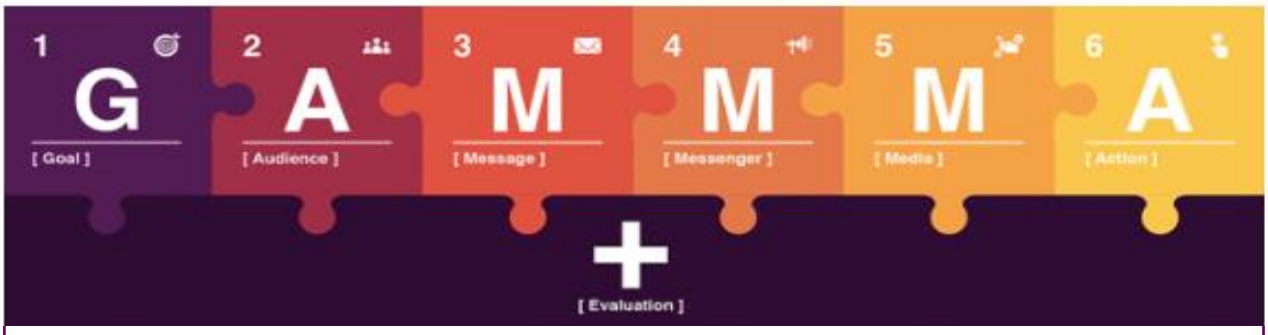
- To credibly communicate after an attack, there should be as small a gap as possible between words and actions. Communications are not the solution to everything, but policies without effective communications may be less effective. We have seen this in recent times, where part of the effective response to the 2019 Christchurch attack rested on its coherence with New Zealand's wider policies towards social cohesion for the last 2 years. Consider the range

of audiences listening to your communications, and in particular how vulnerable audiences might react, as stakeholders will often have to communicate without understanding the full impact of their words. If audiences hear different things from their lived experience, it may come across as inauthentic. **Ensure that crisis communications fit in your overall strategy and narrative.**

- Authorities may prioritise informing the public of the incident and of their approach to investigating it and restoring law and order. In due course, they may choose to condemn the perpetrators and show sympathy with the victims. However, **smart communicators will continue to listen to the public mood and adjust their approach accordingly, as otherwise their approach might potentially backfire**.

GAMMMA+ model

When communicating after an attack, consider the GAMMMA+ model (more information about the GAMMMA+ model can be found here. This provides you with a structured approach to think about the goal, audience, message, messenger, medium and call to action of your communications.



GOAL

What do you really want to achieve? What are your objectives? What is your intervention plan?

- Hone in on your communications goal, and appreciate that it may be different in this context compared to before.
- You may decide to focus on reassuring your audience, promoting unity in the face of adversity, advocating resilience and defiance, etc.
- When we assess the emerging narrative from the event, it may affect the strong counter/alternative narrative to violent extremists required, and it may change between the first 48-72 hours when audiences may be at their most vulnerable, and in the mid/long term as the tone of conversation shifts.

AUDIENCE

What are the key characteristics of your audience? What are they thinking and how do they behave? In what context are they living? What language do they use? Why would they interact with you?

- You will never have as many people listening to your communications as in this post-attack context.
- Your audience is likely to be more general than for traditional P/CVE activities.
- Segment your audience, and tailor your message accordingly.

MESSAGE

How do you ensure that your target audience adheres to your message?

- Keep it simple, maximise impact.
- Do no harm: don't stigmatise vulnerable communities; don't use terrorists' messages, language or imagery.
- Ensure it is credible by being reflective of your actions; consider the nuance required for different audiences.
- Align messages to objectives, but consider prioritising the remembrance of victims, and the promotion of unity at this time, rather than complex or speculative analysis about the causes or motivation of the attack; stay away from the blame game.
- Focus on language, tone and the timing of releases (e.g. cancel other planned releases).
- Take charge of the narrative by creating a common and accessible symbol (such as a hashtag or an image) that can be shared.

MESSENGER

Who are the Messengers that are credible to the target audience?

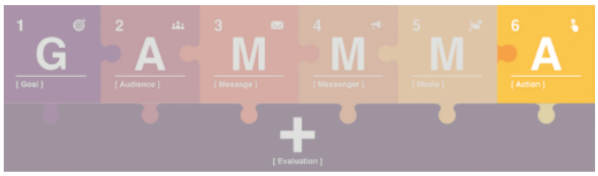
- Work with local and expert stakeholders, who may have better reach, credibility, and therefore influence, than others.
- Be conscious that involving political figures may alienate part of the population.
- By ensuring the right voices are included, with people from different communities and age groups, as well as experts, we build trust and confidence with affected communities in order to believe and support the main messages.

MEDIUM

What Media does your target audience get their information from?

Traditional media opens up as a potential route in the post-attack scenario, because journalists are more likely to be interested.

- Ensure that you have the relevant training and relationships before you engage with the media.
- Ensure that your social media channels are up and running before an incident, and if you have them, use them to communicate clearly and regularly as it will be audiences' most consistent way to gain information from you.



CALL TO ACTION

How could online communication efforts supplement offline work? What is needed for an effective call-to-action? How to get people to act?

- Work together with other stakeholders to find the right action for these communications.
- Ceremonial and symbolic gatherings are important, also for building resilience, but may have diminishing effect after multiple terrorist attacks if audiences feel that they lack substance.
- Try to keep calls to action positive, immediate and easy to achieve.

MONITORING & EVALUATION

How can you measure this and establish that your intervention has made impact? How to best monitor the effect of the call-to-action of your campaign?

- Start monitoring activities as soon as you can after the incident. This will help you understand what the media is reporting, what the position is of each key stakeholder and how your messages are being received.
- Manual monitoring of online, print, TV and radio media can be supplemented with systematic monitoring of relevant chatter on social media.
- After the incident, review your structure, strategy and delivery in a wash-up session to ensure that you can improve your approach for the next attack. Qualitative insights from team members involved in the response can supplement data you will have gathered from your activities.

Further Reading

- Michael Jetter and Jay Walker explore the correlation between media coverage and further attacks: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3286159
- Donald Holbrook writes on the types of media consumed by terrorists: https://icct.nl/wp-content/uploads/2017/09/ICCT-Holbrook-What-Types-of-Media-Do-Terrorists-Collect-Sept-2017-2.pdf
- This RUSI paper on post-attack framework communications: https://rusi.org/publication/other-publications/towards-framework-post-terrorist-incident-communications-strategies
- The Global Coalition against Daesh dictionary, which advises journalists and other stakeholders on doing no harm with language: https://theglobalcoalition.org/en/counter-daesh-dictionary/
- The Words Matter campaign from the Peace Foundation, urging responsible reporting: https://www.peace-foundation.org.uk/terrorism-survivors-urge-media-report-responsibly-following-terror-attacks/
- The Guardian's policy on reporting on terrorism: https://www.theguardian.com/commentisfree/2017/jun/09/reporting-on-terror-without-feeding-it
- IPSO guidance on reporting major incidents: https://www.ipso.co.uk/media/1713/major-incidents-ed-and-journ.pdf
- OFCOM broadcast guidance: https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code/section-three-crime-disorder-hatred-abuse
- BBC guidelines: https://www.bbc.com/editorialguidelines/guidelines/war-terror-emergencies
- The Survivors Assistance Network, a UK NGO that provides support for those who have experienced an attack: https://www.peace-foundation.org.uk/support/survivors-assistance-network/
- Belfast University produced guidelines for media who are interviewing those who have experienced violence, as part of a wider project looking at the Northern Ireland conflict: https://justicehub.org/article/guidelines-for-media-on-interviewing-victims-and-survivors/
- Belfast University also provided guidelines for victims and survivors to consider when speaking to the media: https://pure.qub.ac.uk/portal/files/165825722/Essential_Tips_for_Victims_and_Survivors.pdf
- Some further advice on taking precautions when reporting on terrorist activity: https://www.csa.fr/Arbitrer/Espace-juridique/Les-relations-du-CSA-avec-les-editeurs/Codes-de-bonne-conduite-et-textes-de-precautions-relatives-a-la-couverture-audiovisuelle/Precautions-relatives-a-la-couverture-audiovisuelle-d-actes-terroristes

- And finally, the SAFE-COMMS Terrorism Crisis Communication Manual for Public Authorities, March 2011: https://faculty.biu.ac.il/~sshpiro/pdf/SAFE%20COMMS%20Manual%20final_en_0605.pdf