CENTRIC

Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

Best Practices | Co-Creation | Research

European Network of Law Enforcement Technology Services

CENTRIC Workshop Summary: Insights and Outcomes from the ENLETS Event, October 11, 2023

Alerting and Engaging Citizens in Crisis Response via New and Open Communications Channels while Mitigating Information Overload

Introduction

This discussion paper represents the workshop carried out by CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence, and Organised Crime Research) during the ENLETS (The European Network of Law Enforcement Technology Services) face-to-face meeting at the UK's Home Office premises in London on 11 October 2023.

Having representatives from several law enforcement agencies who attended the event paved the way for the workshop to tap into significant experience and knowledge to shed light on the following goals:

- Increase collective understanding of the capabilities for alerting and engaging citizens; and detecting events and threats whilst managing information overload.
- Establish insight into the next steps towards building and/or employing such solutions, including potential use cases and considerations, and reference to existing solutions.

Having little more than forty-five minutes of discussion during the workshop, the following presentation is not expected to be fully accurate and final. Rather, it is intended to highlight the points, comments and ideas raised during the gathering.

Alerting and Engaging the Public

Informing the public during an incident or crisis is a crucial necessity of a first responder's duty of care. This is carried out not only with the intention to inform, but also to prevent and mitigate risk and harm to the public and their properties. In a predictable setting, the public would be informed both before and after an incident takes place.

Assuming this approach ahead of time is more oriented towards risk assessment and mitigation.

Efforts related to public information may include information campaigns on likely threats in a particular context, for example regularly educating those living in flood-prone areas about local resilience and response plans. Keeping the public, especially the immediate community likely to be affected by the perceived threat, is likewise empowering the community to build their own resilience, which in turn can potentially reduce the scale of an incident's destructive impact.

Once an incident takes place, the focus switches to communicating in a transparent and reassuring manner where possible. At the earliest stage, this may instil confidence in the public that the incident is being dealt with and that help is coming. Such messaging may be a simple reiteration (or nudge) of previous messaging, perhaps reminding the public of what they are expected to do. What seems to be the most important here is that communication is clear, concise, and regular, ensuring that there is a consistent ongoing response and that the public feel that this is truly the case. They should not feel abandoned.

Different types of information may also be sent to different groups of people who assume diverse roles and purposes in the society, and immediately, in their communal environment. The general message may emphasize that the incident is being dealt with and what is expected of people. Targeted messages may provide a call to action (or activation) of other groups that have their own duty of care or mechanisms to assist in pre and post incidents, such as community resilience forums, community groups, volunteer organizations (i.e., mountain rescue), youth groups, local authorities, and highways agencies, to name a few. Each of these groups may have useful contributions to make that can be planned for and then activated during an incident. Information may be as simple as propagating messages within their networks, and as complex as assisting a major incident ahead of (or complimenting) actions to be undertaken by first responders.

When there is a systematic consideration of informing groups (or organizations), this relieves some pressure from the overall alerting system as these groups themselves may be empowered to take control over some element of the response. The more robust pre-incident planning is, the better equipped first responders are. Likewise, better informed public groups may further complement the existing response efforts, and even likely be coordinating together through an agreed communication tool. The wide availability of "good Samaritans" during a complex incident has been seen, but this can be difficult to manage, especially for organizations that directly facilitate the response on the situation while mitigating its impact (serious flooding in the Netherlands was referred to as an example in the workshop).

There are many channels that can be used for both communications and coordination, each with their own advantages and disadvantages. The simplest of these are those focuses on rapid outbound messaging such as email, short messaging service (SMS), and social media. Modern national alert systems that trigger from cellular towers are powerful and cover wider areas but are limited to being a one-way form of communications channel; therefore, such channels are likely most useful in more serious situations, such as widespread disasters, missing persons, and manhunts.

One interesting opportunity discussed is a regional or city-wide "status page" like that of an Internet Service Provider that displays current and ongoing incidents with live updates from response coordinators.

More localized incidents warrant more targeted channels, potentially, and at best, supporting a two-way communications platform. This can range from interesting usages of existing two-way channels such as email, SMS, and social media, to a fully bespoke system supporting end users via a dedicated website or mobile app. Both these approaches can be combined and may complement potential requirements of such a solution that had been discussed later in the workshop.

Some immediate challenges of informing the public were also discussed. It is important to note that in some cases messaging needs to be tightly controlled to avoid creating a negative response and/or unwarranted perception on the scenario or information being dealt with. This may include bad actors utilising the messaging for their own personal gain. Another example would be the response of citizens to assist with good intent, which can be overwhelming and too diverse from the intended mitigation response, thus difficult to coordinate. Even without engaging citizens, there can still be further complexities when coordinating with groups and organizations.

The first responder's duty of care over the public has been emphasized throughout the course of the discussion, whereby in responses undertaken by authorities, the public should not be placed at further risk. Another consideration discussed was the possibility of the alert itself putting citizens at risk, consider a phone going off whilst trying to remain hidden during a terrorist incident.

Situational Awareness and Information Overload

Increasing first responder situational awareness before and after an incident by utilising a wide array of sources including social media may enhance response effectiveness.
However, this must be balanced as the likelihood of information overload may occur, especially while first responders are in action. This can only be achieved by carefully planning all aspects from selecting the right data sources, to appropriately processing, aggregating, triaging, and verifying the data.

When thinking about which data sources to use, this topic is often referring to open-source data, such as social media. A major issue discussed is the rapidly changing landscape of social media, especially a fanning out from what used to be a small number of major suppliers, to now being an explosion of smaller services. In the earlier days of social media (the "golden age of open-source intelligence") the services were more open and encouraging of building solutions on or with their platforms. This has been gradually changing over the last five years or so with online services, including search engines, more tightly locking down access and taking away APIs (or putting them behind paywalls). This shift can be thought of as a transition from platforms (provided to be built upon) to services (provided as is).

The view of content a user has on a social media platform is being even more personalized or curated, making it difficult and sometimes impossible to even search for content anymore. Some social media services now use entirely non-standard technologies (e.g., mobile apps, games consoles) as opposed to more open technologies such as HTTP and HTML. This is making it more and challenging to "listen in" with the assistance of automation.

With these considerations in mind, it is still possible to "listen in" to a point. This just requires defining a clear strategy based on what is available, and what can be "latched" onto within the services, such as widely used or well publicized hashtags (i.e., @MetCC or #MetCC).

Once there is content flowing in, there is a lot that can be done using automation (and artificial intelligence). This is contentious though as there is a strong argument for any decision-making being made by humans alone. Therefore, any automation should be used for purposes of supporting decisions, not making decisions, especially amid the conduct of risk mitigation and response. This can consist of automatically interpreting and categorizing content ahead of a human operator, and perhaps including the identification of relevant objects (or triggers) within text or images.

Then, to help mitigate information overload, there should be some process of aggregation or federation to compress similar content into a single item (some suggestions being by event, location, and time). Then there may be a first-pass triage based on the detected qualities to prioritize which items are presented to the operator first. Based on the experience of those in the workshop, however, it appears that not all these steps are necessary to deliver operational value, considering that some first responders already perform this task effectively with a handful of human operators.

Being able to verify the content and any information fed to first responders is not only very important but is also an area of complexity and uncertainty, to a certain extent, at this time. While there is significant research being undertaken in misinformation and disinformation, it is likely that it will take some time before automation can be effectively used on a general basis, especially those with novel content, at a level that will satisfy the needs of first responders. This said, when discussed in the workshop, there was a recognition that this really is something that is already being managed all the time. The issue of validity is already a concern with emergency phone calls, alongside misinformation and disinformation that do occur and are managed. The same is currently true where social media is being utilized in first responder communications centre. While it cannot be denied that a lot of unreliable information does come in and is reported to various first responders' monitoring channels, these are taken on face value to satisfy the duty of care requirement – "what if it's true?".

Other considerations were also raised. Firstly, whilst there is the risk of misinformation, there is also the risk of receiving too much conflicting information. In a complex situation, this may lead to an ineffective and confused response. There is a recognition that "you'll never get exactly what you want, you either get too little or nothing, or you get too much, and you can't handle it." First responders, and even those in the communications centre, face a situational dilemma where their action meets their duty of care – "Is this not better than doing nothing?". There have been cases where information (and the conversation) online can lead to further harm, such as vigilante groups targeting a potential suspect.

The bottom line is that the risk of information overload should not be an imperative to do nothing.

Existing Solutions

Some existing solutions that address all or parts of that discussed here were raised in the workshop. These include:

- **GoodSAM** [1]: Crowdsourcing resuscitation of cardiac arrest victims by tapping into a network of medically trained volunteers.
- **Burgernet** [2]: (The Netherlands) Issuing actions to registered volunteers via mobile app or email, including looking out for a person or vehicle, asking for witnesses, and alerting users to a suspicious or unsafe situation. Also includes Amber Alerts (i.e., missing persons).
- **Amber Alert EU** [3]: Focussed on missing children, it also provides a list of solutions in European Union countries that may cover this responsibility and others discussed here.
- **ATHENA** [4]/**SCAAN** [5]: Presented during the workshop session as an example of technical solutions with partial coverage of the discussed use cases, as below.
  Several further solutions, or parts of solutions, were also mentioned during the workshop session.

Use Cases Considerations

Several use cases were mentioned or can be derived from the workshop discussion, these include:

- **Alerting/Disseminating Information:** To send alerts to citizens (e.g., risks, dangers, instructions), so that they can be better informed and can react according to official guidance.
- **Request Volunteer Information:** To send requests for information to citizens (e.g., witnesses, bystanders, victims and their immediate social circle, observations of person or vehicle, verification), so that situational awareness by first responders can be increased, allowing more effective planning and response.
- **Request Volunteer Assistance:** To send requests for specific assistance to citizens (e.g., first aid, cardiopulmonary resuscitation [CPR], translation) so that the response can be faster and more effective by utilizing a larger and more dispersed pool of potential resources.
- **Allow Volunteer or Public Reporting:** To allow a network of volunteers (or the public) to easily submit information (examples are sightings, observations, insights, concerns), with intent of reducing risk of a late or no report of a developing or occurring risk or threat by empowering citizens to easily report anything and without fear of repercussions.
- **Coordinate Response and Stakeholders:** To allow hierarchical coordination of a situation, including handover and delegation across multiple organizations and entities, so that the relevant authority has the appropriate control and situational awareness across all aspects of the response.

A shared goal of these use cases is to increase transparency and to give reassurance and authoritative guidance to the public as efficiently as possible.

Further Considerations

These considerations were discussed or can be derived from the workshop:

- Can a solution be delivered by both commercial and non-commercial means (i.e., government)?
- Can the existing systems be more broadly adopted by other countries?
- Can the existing systems be brought together or integrated in some way?
- Can communication channels (i.e., public broadcasting systems) be mandated for this purpose?
- Can the duty of care to deliver some components or services be placed on relevant organizations (i.e., public broadcasters)?
- Can parts of the solution be mandated on device manufacturers (e.g., Apple, Samsung)?
- Can the solution utilise both consumer-level (i.e., SMS, email) and infrastructure-level (i.e., cell tower alerting) mechanisms?
- Can cross-network functionality be mandated (such as how 112/999 is currently available on all networks and when roaming)?
- Can the solution utilise existing operational mobility and standardization approaches (i.e., BroadNet [6])?
- Can strategic and operational plans be identified at an early enough stage to ensure consistency and compliance across all relevant authorities and organizations?

Next Steps

Again, this discussion took place in less than forty-five minutes of the allocated time. To take this forward, below are some key areas of the activity that can be identified now.

There should be a deeper exploration of the different use cases and scenarios that the proposed solution may address, and to identify any gaps and potential advantages a new solution may have over existing processes that cover these. Such proposal should also include engagement with international partners that are utilising the existing solutions as discussed here to understand any gaps they have, and whether they can be deployed as is (or with little work).

As part of this work, there should be some development of clearer requirements for the above use cases that each relevant authority may have, especially with regards to integration. Other stakeholders, organizations (e.g., voluntary, non-governmental) as well as citizens may be included in the discussion to better establish their role within the solution, and thus, their requirements. It is also important to establish which of these use cases (and therefore requirements) are critical by using a standardised prioritisation approach (i.e., MoSCoW [7]).

At this stage, drafting operating procedures that make assumptions about the functions and interfaces of the workshop's proposed solution may also be developed to encourage a cohesive approach between the use cases and all relevant moving parts. Developing user scenarios or stories will be helpful for further establishing what these procedures may look like. More detailed technical requirements may also be drawn from these new resources.

References

[1] https://www.goodsamapp.org
[2] https://www.burgernet.nl
[3] https://www.amberalert.eu
[4] https://cordis.europa.eu/project/id/313220
[5] https://scaan.app
[6] https://www.broadway-info.eu/broadnet-preparation
[7] https://en.wikipedia.org/wiki/MoSCoW_method

CENTRIC: Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

centric@shu.ac.uk

research.shu.ac.uk/centric/