

The use of shared digital platform solutions to address challenges to multi-agency preparedness, response and recovery work within the UK

Received (in revised form): 26th May, 2023

Laura Drew

Public Health Senior Emergency Planning Officer, Kirklees Council, UK

Laura Drew started in the emergency planning industry by studying for a bachelor's degree in emergency and disaster management and a master's degree in emergency planning and management at Coventry University. She subsequently worked for a private consultant, for whom she started up business continuity services to both public and private sector. She subsequently assumed the roles of Emergency Planning Manager for West Midlands Police, and then Public Health Senior Emergency Planning Officer in a local authority. In 2012, Laura was awarded the UK Emergency Planning Society 'Resilience Planner of the Year' and the West Yorkshire Police Women in Policing Award for 'Excellence in Performance'.

ABSTRACT

This paper discusses ResilienceDirect — the UK's strategic resilience platform for response and information sharing, designed to support the multi-agency aspects of emergency response. The paper will focus on the functionality of the system as well as the related challenges. The paper identifies a set of recommendations for addressing the challenges to improve usability and uptake. The recommendations will consider best practices from other multi-agency response platforms and feedback from ResilienceDirect users.

Keywords: *ResilienceDirect, interoperability, emergency response, resilience, JESIP, communications*

BACKGROUND

The UK emergency response system is legislated via the Civil Contingencies Act 2004. To help those responsible for complying with the requirements of this act, the UK government has published guidance documents with a focus on both emergency preparedness and emergency response and recovery. These documents focus on the delivery of multi-agency responsibilities under the act, and identify seven key duties (five main and two supporting) to ensure the implementation of an effective response system. The Cabinet Office¹ identifies the five main duties as risk assessment, business continuity management, emergency planning, warning and informing for public awareness, and advice and assistance to commercial and voluntary organisations (the latter being for local authorities only). Further to these, 'the Act then adds two more duties for the Category 1 responders. They are required specifically to cooperate and share information in delivering the other five duties'.²

UK agencies that are required under statute to be involved in multi-agency preparation for, response to and recovery from emergencies are split, under the Civil Contingencies Act,³ into two main categories (Category 1 and Category 2). There is also a non-statutory third sector, which is highlighted in reference to support



Laura Drew

Kirklees Council,
PO Box 1720,
Huddersfield HD1 9EL,
UK
E-mail: laura.drew@kirklees.gov.uk

Journal of Business Continuity
& Emergency Planning
Vol. 17, No. 2, pp. 187–198
© Henry Stewart Publications,
1749–9216

agencies that may be able to support the Category 1 and 2 statutory authorities. These categories include a wide range of organisations with diverse statutory and non-statutory duties (see Appendix A). The Kerslake Report⁴ identifies that ‘emergency preparedness, response and recovery in the United Kingdom are built on the concept of delivering multi-agency integrated emergency management ... through a process of collaboration, communication and coordination between agencies and organisations’. This again demonstrates the need for communication to support activities specific to cooperation and information sharing, as per the Civil Contingencies Act.

One way that the UK aims to promote this multi-agency response in day-to-day business is via the implementation of local resilience forums. As specified by the Cabinet Office,⁵ a ‘local resilience forum is the principal form of multi-agency cooperation in a local resilience area’ based on police force areas. The local resilience forums support this cooperation by providing a forum to act as ‘the principal mechanism for multi-agency collaboration and coordination’.⁶ At the time of writing, the Cabinet Office⁷ identifies 42 local resilience forums across England and Wales.

In addition to the local resilience forums, a set of principles has been established to help manage the multi-agency response aspects of a response known as Joint Emergency Services Interoperability Principles (JESIP). JESIP was put in place to rectify issues such as interoperability and communication failure, previously identified in larger-scale historic responses, such as the 1987 fire at Kings Cross station, in London. With learning from such historic responses in mind, JESIP has been implemented as a national programme⁸ by agencies that respond to emergencies, and it aims to better ensure organisations can

work together and save lives by improving interoperability and communication across all levels of a response. The programme has put in place a joint doctrine, along with other supporting documents, outlining principles and protocols concerning joint decision making,⁹ sharing of learning from exercises and incident response,¹⁰ and setting shared situational awareness templates (eg M/ETHANE templates¹¹).

MULTI-AGENCY RESPONSE CHALLENGES

From the background of multi-agency response already discussed, it is possible to see that multi-agency working is an important and integrated practice in UK emergency response. One can also surmise that by its very nature, multi-agency response involves numerous different organisations, with differing levels of expectations and responsibilities outlined under the Civil Contingencies Act. The Cabinet Office¹² identifies that cooperation can ‘be facilitated through outward-facing, structured communications methods’. It further adds that ‘information sharing is a crucial element of civil protection work, underpinning all forms of cooperation. Category 1 and 2 responders should share information formally and as part of a culture of cooperation’.¹³ From this, it is possible to derive that such a practice will require effective communication, particularly around information sharing, to ensure a coordinated, effective and timely response to emergencies.

The more organisations involved, the greater and more complex the requirements around these factors will be for each organisation. This is further impacted by the nature of the response requirements and pace at which the situations develop. The Risk and Resilience Hub¹⁴ supports this by identifying that any system in place to support a multi-agency response

‘community will work only if you and others get involved’. This is particularly the case for communications and information sharing in that if key agencies are not present on the system being used, they will miss out on what is being shared and be unable to provide what may be required, resulting in an incomplete situational picture. Tracplus¹⁵ supports this need to have access to the same systems and same information, noting that ‘to ensure the best emergency response, a single data set, in a common format, is vital’.

Recent UK emergency responses, debriefs and other responses analysed have shown that communication and information sharing remain an issue, especially in the early stages of response. For example, following the inquiry into the 2017 suicide bomber attack at Manchester Arena, the Kerslake Report¹⁶ identified challenges for ‘partner agencies for not sharing additional information (including clearly defined M/ETHANE messages and major incident notifications) [when] ... communication of such information is after all a key requirement within the JESIP principles’. Specifically, there was an issue where ‘there was not a shared communication across the agencies of the declaration of Operation PLATO, which is the agreed operational response to a suspected Marauding Terrorist Firearms Attack, nor was there a shared understanding of its implications’.¹⁷ This clearly indicates a need for good communications and information sharing to better ensure a shared understanding of response requirements and of the incident implications to help join up and ensure a more effective and efficient multi-agency response. The faster this can be established, the earlier in the response a joint understanding can be developed and timely multi-agency response can commence.

The Kerslake Report also underscores the need to ensure that all elements of

response are demonstrable. It identifies that:

‘Officers who attended the Command Support Room had been in telephone communication with each other and others ... However, the Panel finds it hard to conclude that such communications between individuals enabled this group of senior officers to establish a shared situational awareness and joint understanding of risk to any substantive degree until they physically arrived at the building’.¹⁸

It is essential to log or document any information being shared in order to provide a record that responders can consult should they need to clarify their understanding of the situation. While such checks may be carried out via verbally (ie by seeking clarifications from other persons), responses may differ from original communications if not delivered by the same person; even then, hindsight can impact how information is interpreted as an incident progresses.

In this respect, similar shortcomings were identified in the phase 1 report on the Grenfell Tower Block fire that occurred on 14th June, 2017 in North Kensington, London, and in which 72 people died. In relation to the government response, the report¹⁹ identified a failure in communications and information sharing, as indicated in its recommendation ‘to improve the communication arrangements between the three emergency services, their respective control rooms, and the incident ground ... [to improve] joint working, improve shared situational awareness and [provide] a joint understanding of risk arrangements’.

The summary of the phase 1 report²⁰ highlighted that one of the major issues in the multi-agency response was the agencies’ failure to communicate the

declaration of a major incident. This was identified to be:

‘A serious failure to comply with the joint working arrangements and protocols designed for major emergencies in London ... [the consequence of this meant that there was] ... a lack of shared understanding of the nature and effect of the fire ... [and that] ... conversations that should have taken place between the supervisors of the different control rooms did not happen’.

From the above, it is clear that any tool to support multi-agency response must:

- Be able to support the communication of situations (eg via situation reporting, agency updates, etc.);
- Ensure timely communications;
- Be accessible at both operational scenes and from within command centres/responder base locations to ensure the full hierarchy can see the shared information and feed into such information as appropriate to ensure the provision of a shared situational understanding; and
- Provide information in a written/visual form so that there is not only evidence of the message being passed, but also so that anyone can revisit this in a timely fashion to clarify positions and understanding around an emergency and the connected response.

ADDRESSING UK MULTI-AGENCY RESPONSE CHALLENGES: RESILIENCEDIRECT

To assist in preparing for an emergency response, the UK government developed an online platform known as ResilienceDirect. This system is now being used across the UK by multiple agencies to aid in their preparation for, response to and recovery from emergencies, while

allowing real-time information sharing and joined-up communications. It can be used during a response, via the incident response pages function; to date, however, it has been found to work more effectively in response to slower-paced incidents (eg Brexit, COVID-19, etc.) than with rapidly evolving incidents (eg the Manchester Arena attack).

Under the Civil Contingencies Act, any UK organisation that qualifies as a Category 1 or 2 responder status is entitled (indeed, encouraged) to access the full version of ResilienceDirect. Therefore, accounts are held by a variety of single agencies (such as those identified in Appendix A of this paper) as well as multi-agency bodies/groups, such as local resilience forums. The Cabinet Office²¹ requires Category 1 responders to ‘encourage organisations which are not covered by Part 1 of the Act to cooperate in planning arrangements’. To support this, ResilienceDirect allows Category 1 responders to sponsor local organisations for ‘lite’ accounts. This facilitates the sharing of information and involvement of other organisations where appropriate (this includes local control of major accident hazard sites, rest centre sites, etc.). In areas with well-supported sign-up, this provides an opportunity for very effective information sharing and wider emergency response interaction to create a well informed, commonly recognised information picture.

ResilienceDirect offers a variety of functions to support emergency response, including helping to address the efficiency of multi-agency response by providing a space to support information sharing and incident response processes. The functions of ResilienceDirect that assist in this include the following:

- *Mapping hub*: ResilienceDirect supports the creation of shared maps that can be updated in real time by authorised

organisations/accounts, in addition to static layer upload and management, live RSS feed layer upload and management, etc.;

- *Collaborate hub*:
 - ResilienceDirect supports an evolving incident response page with templates for the development and sharing of situation reports at both tactical and strategic level, in addition to agency report updates supporting red, amber, green (RAG) status allocation to response needs and forward-look elements; an incident log that supports the assignment of tasks to specific people by generating an e-mail to those people, and allowing task management and updates to be added; and the ability to add other areas, such as document-sharing repositories, and links to plans or maps on other areas of the system, etc.;
 - Organisational pages are provided for the sharing of information such as plans and other supporting documents (eg guidance and risk assessments, mutual aid or other pre-arranged resource agreements); templates for organisations to use during a response; and forums for the sharing of debrief reports, information regarding training and exercises run, and meeting documents (eg agendas and minutes), etc.;
- *Cyber hub*: This is a preparedness platform rather than an active response area and as such is used for sharing toolkits, good practice, threat updates, national training and exercising for use at organisational level, etc.;
- *Learning and development hub*: This is a platform to allow those working in the field of resilience to stay up to date with best practice and access JESIP's joint organisational learning platform for sharing learning from incidents and

exercises to allow the wider sharing of lessons learned from exercises and incident responses.

As per the challenges previously identified in recent responses around communication and information sharing, ResilienceDirect offers the following solutions:

- Incident response pages include a M/ETHANE (situation) report. Incident pages also include a red banner for important headline updates at the top of the page (this could help address the issue of getting key messages to all agencies such as incident type/designation issues);
- ResilienceDirect is quick to set up for use in an incident, which would help address timeliness of ensuring joint situational awareness. This further supports a need highlighted in the Kerslake Report,²² namely that 'it is essential that this communication across the agencies happens and happens early';
- ResilienceDirect allows all those with an account access to the shared information picture, no matter what level in the hierarchy they are. So not only is it a shared multi-agency picture, but it also allows for a shared hierarchical picture internally within response agencies.

ISSUES AND CHALLENGES OF RESILIENCEDIRECT

One of the main challenges to the effectiveness of ResilienceDirect relates to the level of sign-up across and within organisations that may be required to respond to emergencies in a multi-agency capacity. As part of this paper, a survey on the use of ResilienceDirect (see Appendix B) was issued to those working in the multi-agency emergency response environment. Ninety-four per cent of respondents reported that their organisation had a

presence on the ResilienceDirect system; in other words, 6 per cent have no presence on the system. Furthermore, those with a presence identified that only select teams held access (with 80 per cent of this being limited to emergency planning related teams/roles only, due to them being the lead for emergencies and the logical lead and administrator for their respective organisation's system). This indicates that key organisations or key internal roles within the information sharing and incident response process remain excluded from ResilienceDirect during incident response and are unable to share their own updates as part of the information and response process. This results in a gap in the wider response picture.

The extent to which ResilienceDirect is used within individual organisations is a further factor, with differences in practice becoming an obstacle to the smooth transition of the system from single use to multi-agency use. The results of the survey indicate that different organisations use ResilienceDirect to a different extent as follows:

- Information and file sharing (externally): 57 per cent;
- Information and file sharing (internally): 48 per cent;
- Incident response: 57 per cent;
- Exercises: 57 per cent;
- Accessing information from other organisations: 52 per cent;
- Mapping: 38 per cent;
- Joint organisational learning: 38 per cent; and
- Business continuity: 5 per cent.

The areas where these differences in usage are most acute are most likely to be the areas where there are challenges during multi-agency emergency response. These challenges include breakdowns in communication between different parties and

challenges to the effective sharing of information. When not all who require access to information can access it and not all those who need to share it, can share it, this impacts negatively on multi-agency work. Such a situation may also lead to the sharing of information via unofficial channels, resulting in things getting lost in the system, and people working according to outdated information, etc.

The overwhelming majority of survey respondents indicated that ResilienceDirect was fit for purpose for multi-agency response, identifying the following as areas that ResilienceDirect does well:

- It expedites the sharing of information between users without the need to call or e-mail people;
- Mapping provides a good visual of key locations to assist all users with access a joint understanding of locations, the geography of affected areas, etc.;
- It supports collaborative working between categorised responders in a multi-agency manner via a single platform for activity, rather than spreading that activity across numerous organisational systems that do not allow users talk to each other;
- It offers good disaster recovery options for accessing plans and other documents stored on the system when organisational network access is lost;
- It is a free-to-use platform that provides organisations with a solution to meet the Joint Emergency Services Interoperability Principles and multi-agency requirements of the Civil Contingencies Act;
- It has an alert function to get messages out to selected users quickly based on pre-built lists (ie based on page access authorisations).

While 86 per cent of survey respondents indicated that ResilienceDirect was fit for

purpose for multi-agency response, 14 per cent reported it as inadequate. When respondents were asked why felt it was not suitable, they identified various issues relating to willingness to use, usability and actual ability to support multi-agency needs, including the following:

- ResilienceDirect is seen as an emergency response tool, hence there is a perception among those working outside that responsibility is that it is not for them. This makes buy-in challenging;
- Most organisations already rely on an extensive suite of software, and potential users are reluctant to add another to the list;
- The platform is not end-user driven in its design: it is not simple to use and feels clunky to users;
- The existence of platforms like Microsoft Teams that are both easier to use and more frequently used poses a challenge to organisational buy-in across a wide user footprint;
- As ResilienceDirect is not a day-to-day system for most people, the infrequency of usage can result in users becoming deskilled and losing confidence in their ability to use the system. Related challenges include finding time to train users who work out of hours and competing pressures on people's time preventing them from being able to attend training or practice exercises;
- Usernames are complicated and hard to remember, with the result that users are often locked out. There is no local option to reverse this, and such issues must be referred to the Cabinet Office support team (who do not work out of hours). This is highly problematic when incidents occur outside of office hours and access is needed as soon as possible;
- Mapping is very visual, with no ability to download data into a readable format for further analysis. Thus, only a portion

of user needs relating to mapping can be met;

- Non-categorised organisations with 'lite' accounts have very limited access. For example, they can view only what they have been authorised to see and cannot maintain their own pages to share their own information;

If the effectiveness of multi-agency response is expected to improve through better inter-agency communications, and an improved information picture, these challenges must be addressed.

OTHER EXISTING OR PROPOSED MULTI-AGENCY RESPONSE PLATFORMS

'Emergency response providers are looking for platforms and software to provide solutions which mitigate historical issues when mobilising multiple agencies — issues such as communication breakdowns between agencies, and a lack of situational awareness'.²³ As ResilienceDirect is by no means the only system of its kind, what are some other examples we can consider in addressing multi-agency response communication and information sharing?

Universities in the UK are developing options for multi-agency response systems to aid communications and information sharing between emergency response partners. The University of Salford has devised a platform called Mobilise, which it describes as a:

'Web-based digital platform that allows distributed intelligence from various organisations and devices (satellite, sensors) to be brought together to understand the vulnerabilities, slow onset disasters, rapid onset disasters in an area and use that knowledge to take collective actions to reduce disaster risks as well as response better to disasters'.²⁴

The system, like ResilienceDirect, can offer both peacetime (eg preparedness and mitigation support tools) and emergency response (eg information sharing) options. This system²⁵ offers such features as three-dimensional visual data; simulations to predict people movement during an emergency; a community resilience measurement tool; tools to generate information to assist decision makers based on simulation and information feeds; a touchable interface allowing for intuitive use; a team-centric interface to support multi-agency usage; and an early warning system. The system also offers the potential basis for the implementation of an algorithm to process incoming intelligence and data, alongside existing data, to support better-informed decision-making by understanding the range of possible outcomes of those decisions.

The University of Surrey has also considered a similar platform, known as Distributed Autonomous and Resilient Emergency (DARE). This emergency management system has been designed to be able to provide ‘an effective and efficient critical communication platform that provides situational awareness and coordination’.²⁶ The DARE platform has thus been designed to consider system resilience due to current platforms being

‘Susceptible to being incapacitated or destroyed by the disaster or the network congestion that arise as a result of such disaster ... [as such the design was based] ... upon three main communication platforms that are wireless sensor networks (WSNs), *ad hoc* networks and future cellular networks (5G and beyond)’.²⁷

This underscores the importance of building resilience into the design of emergency management systems, and of considering the different options when it comes to connections and communication platforms.

Outside of the university sector, private organisations have also developed software and cloud-based options that can be used for emergency response and resilience. Two notable examples are Crisis Commander²⁸ and Mission Mode.²⁹

Crisis Commander is a cloud-based system that caters for many emergency preparedness and response needs. It allows the on-system development of plans but also uploading of other formats of existing plans. By developing these plans on the system or uploading in certain formats, an interactive checklist can be activated during times of response to help coordinate and capture response actions. This system also comes with an app, specifically configured for phones and tablets, to support access to and management of the system. As part of the response system, it is possible to allocate tasks to individuals. Those individuals are notified via e-mail, but also via SMS and phone push notifications. In these notifications, a link to update the tasks is provided, regardless of account status on the system. It is also possible to customise the view of individuals based on their roles (eg show only action cards applicable to them, show only report templates and levels of information applicable to a role, etc.).

Mission Mode is also a cloud-based incident management system with emergency notification capabilities. This system allows for incident logging, plan development, task allocation, resource allocation, etc. Like Crisis Commander, the system can be accessed via an app to allow more streamlined on-the-go management, which is a benefit during a response, especially for operational responders deployed on scene/remotely from control centres. The system also allows for instantaneous automated messages to be sent to pre-identified contact lists, as well as for two-way communication using forms, text, checklists, images and GPS location services, even when voice and SMS are not working.

Clearly, both Crisis Commander and Mission Mode have some good functionality that could inform further development of the ResilienceDirect system. As systems in themselves, however, there are certain things that they cannot offer that ResilienceDirect does. Both Crisis Commander and Mission Mode require a subscription fee and are organisation-specific platforms. Information can be shared with those outside the organisation, but the systems do not support the joined-up response of a multi-agency environment. This said, however, there is potential for them to work well in a control centre where those within the room can input all the logs and data required, and tasks allocated can be viewed on shared screens by a host organisation. In this respect, ResilienceDirect is more streamlined for real-time response.

PROPOSED IMPROVEMENTS TO RESILIENCEDIRECT

As part of the survey on the use of ResilienceDirect, respondents were asked for suggestions on how to increase adoption of the system and how to make it more effective for multi-agency response. The following recommendations were made:

- Improve the interface to make it more intuitive, less intimidating, and easier to navigate (eg by providing one-click access to key areas);
- Investigate whether ResilienceDirect could be run via Office 365 to get buy-in from wider services;
- Adopt simpler logins to reduce the risk of lockouts during incident response (or use single sign-on authentication connected to organisational Office 365 accounts);
- Develop an app-based login option for mobile devices (also supported by looking at what other emergency response and resilience platforms can offer);
- Mandate use for categorised responders to ensure a minimum standard for sign-up is achieved and help minimise the risk of gaps in the information picture or certain organisations not getting information;
- Provide train-the-trainer sessions to empower different organisations and agencies to deliver training to the same standard, so that all users share an equal understanding of the system;
- Increase usage ability for 'lite' account holders, so they can share information from their own pages;
- Allow data downloads from mapping so that information can be downloaded in a readable format for further analysis (rather than having to click into each feature and note the information pertaining to that point, which is time-consuming when having to access multiple data points);
- Involve users in the updates being made and ensure full warnings and details around updates are communicated to users in a timely manner;
- Add a secure page option that does not inherit parent page access, and make the security and setup of pages more straightforward from an administrative point of view;
- Design off-the-shelf multi-agency exercises so that organisations can practise using the system more regularly;
- Implement a national standard for file structure within organisational pages so that when accessing the files of external organisations, it is clear where to find the information required. Likewise, introduce a template for incident pages to ensure all essential information is captured in a uniform manner, again making it easier to navigate pages hosted by alternative agencies;
- Consider the introduction of a resilience

standard based around ResilienceDirect with more onus on the role of local resilience forums as the overarching multi-agency body for their respective geographical locations, and the importance of their role in the development of multi-agency arrangements and response options.

In addition, based on what can be observed from other electronic multi-agency response platforms, the ResilienceDirect system would also benefit from the following changes/improvements:

- Improved resilience to network interruptions to better ensure system access in the event of network outages;
- Customisable views for users to tailor their experience so their dashboard is not cluttered with information/systems options that they do not need, especially during an emergency response;
- The extension of availability to all levels of response (ie on the front line, not just within control rooms) — having it available as an app may assist with this;
- The ability to allocate tasks to individuals — whether by SMS, e-mail or push notifications — and for those individuals to post status updates, even if they do not have a credentialed account to log into the system;
- The ability to partake in multi-agency training and exercises;
- The use of algorithms to cross-reference live data with relevant existing data to identify potential outcomes to aid decision making (support for this is shown by Tracplus,³⁰ which comments that ‘software management systems need to democratise the data to provide intelligence to make quick and effortless decisions with status boards showing the real-time location and status of crews, manifesting and two-way voice/text message communications’);

- Shared procedures for the use of functions such as information sharing, mapping, M/ETHANE reporting, situational reporting, agency reporting and logging, in order to improve shared situational awareness through the provision of a more effective visual picture around responder locations, affected locations and the overall risk picture.

CONCLUSION

The UK currently widely uses the ResilienceDirect system as a platform to assist multi-agency communication and information sharing to support coordination both in preparing for and during incident response. As this paper has identified, ResilienceDirect has made good headway in assisting the UK improve issues relating to communication and information sharing. Nevertheless, the system still requires further development to address the challenges faced in multi-agency communications and information sharing more wholly. By means of a survey of ResilienceDirect users and a comparison with similar systems, both existing and under development, this paper has identified some of these developmental requirements, presenting them as a series of recommendations. These recommendations include mandating use of the system, the standardisation of organisational pages, improvements to the system interface, the introduction of a ResilienceDirect app, expanded functionality for lite account holders, and the use of algorithms and data downloads/uploads from live data feeds.

In summary, the paper finds that the UK has a good multi-agency platform in ResilienceDirect, and while it is, overall, fit for purpose, a few adjustments would help drive wider adoption, which in turn would make it more effective in a range of incident response scenarios.

APPENDIX A

Table A1: The categorisation of responders in the UK and their allotted responsibilities

| <i>Categorisation</i> | <i>Organisations this includes</i> | <i>Responsibilities under the Civil Contingencies Act 2004</i> |
|-----------------------|---|--|
| Category 1 | Local Authorities, Emergency Services (Police, Fire and Rescue Service, British Transport Police), Health (National Health Service, NHS Foundation Trusts, Ambulance Service, Health Boards (Scotland)/Local Health Boards (Wales)), Secretary of State, Port Health Authority, Environment Agency, and Maritime and Coastguard | Risk assessment, business continuity management, emergency planning, maintaining public awareness, arrangements to warn, inform and advise the public, provision of advice, and assistance to the commercial sector and voluntary organisations (this final one is for local authorities only) The above is underpinned by the requirement to cooperate and share information and the need to have regard for third-sector support. |
| Category 2 | Utility Companies, Railway Transport Providers, London Underground, Airport Operators, Harbour Authority, Highways Authority, Health and Safety Executive, Integrated Care System, Office of Nuclear Registration, The Common Services Agency (Scotland), Public Health Scotland (Scotland) | Support Category 1 organisations via the requirement to cooperate and share information |
| Third sector | Voluntary sector, military, etc. (not exhaustive) | Support the response based on requests from the Category 1 response |

APPENDIX B

The survey of ResilienceDirect users received a total of 154 responses from people working in emergency response roles within the following types of organisation:

- Local authorities: 89 respondents;
- NHS hospital trusts: nine respondents;
- NHS commissioned organisations: seven respondents;
- Local resilience forums: three respondents;
- Mental health trusts: six respondents;
- Integrated care boards (formally clinical commissioning groups): eight respondents;
- Fire and rescue services: 26 respondents;
- Civil service: six respondents.

REFERENCES

- (1) Cabinet Office (2012) 'Introduction', in 'Emergency Preparedness', Chapter 1, HM Government, London, pp. 1–18.
- (2) Cabinet Office (2012) 'Co-operation', in 'Emergency Preparedness', Chapter 2, HM Government, London, pp. 1–66.
- (3) HM Government (2004) 'Schedule 1: Category 1 and 2 Responders', Civil Contingencies Act, HM Government, London, pp. 1–53.
- (4) Kerslake, B., Wahlstrom, M., Deeming, H., Goodwin, A. and Lund, K. (2018) 'The Structure of Integrated Emergency Management in the United Kingdom: Key Concepts', in 'The Kerslake Report.'
- (5) Cabinet Office, ref. 2 above.
- (6) Cabinet Office (2012) 'Collaboration and Co-operation between Local Resilience Forums in England', in 'Emergency Preparedness', Chapter 16, HM Government, London, pp. 1–6.
- (7) Cabinet Office (2022) 'Local Resilience Forum: Contact Details', available at: <https://www.gov.uk/guidance/local-resilience-forums-contact-details> (accessed 22nd November, 2022).
- (8) JESIP (2022) 'Home Page', available at: <https://www.jesip.org.uk/> (accessed 23rd November, 2022).

- (9) JESIP (2022) 'The Joint Decision Model', available at: <https://www.jesip.org.uk/joint-doctrine/the-joint-decision-model-jdm/> (accessed 23rd November, 2022).
- (10) JESIP (2022) 'JOL Guidance', available at: <https://www.jesip.org.uk/downloads/joint-organisational-learning-guidance/> (accessed 23rd November, 2022).
- (11) JESIP (2022) 'M/ETHANE', available at: <https://www.jesip.org.uk/joint-doctrine/m-ethane/> (accessed 23rd November, 2022).
- (12) Cabinet Office, ref. 2 above.
- (13) Cabinet Office (2012) 'Formal Information Sharing Under the Civil Contingencies Act 2004', in 'Emergency Preparedness', Chapter 3, HM Government, London.
- (14) Risk and Resilience Hub (2022) 'About Us', available at: <https://www.riskandresiliencehub.com/about-us> (accessed 22nd November, 2022).
- (15) Tracplus (2021) 'Technology's role in multi-agency emergency response', available at: <https://www.tracplus.com/blog/multi-agency-management-during-mass-casualty-events/> (accessed 22nd November, 2022).
- (16) Kerslake, B., Wahlstrom, M., Deeming, H., Goodwin, A. and Lund, K. (2018) 'Panel Conclusions: The emergency services — notable practice and lessons identified', in 'The Kerslake Report'.
- (17) Kerslake, B., Wahlstrom, M., Deeming, H., Goodwin, A. and Lund, K. (2018) 'Executive Summary', in 'The Kerslake Report'.
- (18) Kerslake *et al.*, ref. 16 above.
- (19) HM Government (2020) 'Recommendations for all Fire and Rescue Services (FRSs)', in 'Grenfell Tower Inquiry Phase 1 Report: Government Response', HM Government, London.
- (20) Moore-Bick, M. (2019) 'Executive Summary: The response of the other emergency services, RBKC and the TMO', in 'Grenfell Tower Inquiry: Phase 1 Report: Report of the Public Inquiry into the Fire at Grenfell Tower on 14 June 2017 (Volume 1)', HM Government, London.
- (21) Cabinet Office (2012) 'Other sectors that should be involved in Emergency Planning', in 'Emergency Preparedness', Chapter 15, HM Government, London.
- (22) Kerslake *et al.*, ref. 17 above.
- (23) Tracplus, ref. 15 above.
- (24) University of Salford (2021) 'A Collaborative Multi-Agency Platform for Building Resilient Communities', available at: <https://gtr.ukri.org/projects?ref=EP%2FP028543%2F1> (accessed 17th November, 2022).
- (25) University of Salford 'Think Lab', available at: <https://mobilise-project.org.uk/platform/> (accessed 1st December, 2022).
- (26) University of Surrey (2020) 'DARE: Distributed Autonomous and Resilient Emergency Management System', available at: <https://gtr.ukri.org/projects?ref=EP%2FP028764%2F1> (accessed 17th November, 2022).
- (27) *Ibid.*
- (28) Crisis Commander (2022) 'Crisis Management with Crisis Commander', available at: <https://www.everbridge.com/blog/crisis-management-crisis-commander/> (accessed 10th May 2023).
- (29) Mission Mode (2018) 'Mission Mode Solutions', available at: <https://medium.com/@missionmodesolutions> (accessed 10th May, 2023).
- (30) Tracplus, ref. 15 above.

Copyright of Journal of Business Continuity & Emergency Planning is the property of Henry Stewart Publications LLP and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.