

CRISIS▶RESPONSE

VOL:12 | ISSUE:4 | AUGUST 2017

WWW.CRISIS-RESPONSE.COM

JOURNAL

PROTECTION | PREVENTION | PREPAREDNESS | RESPONSE | RESILIENCE | RECOVERY



SPACE TECHNOLOGY ITS ROLE IN DISASTER MANAGEMENT TODAY

Fake news; Radicalisation in Central Asia; Ransomware & cybersecurity; Lindt Café siege; Treating Afghanistan's victims of war; Emergency management & resilience; Artificial Intelligence; 3D printing technology; Drones & EENA; Computer modelling in large scale incidents; The impact of NIMS; Robotics for good

Editor in Chief
Emily Hough
emily@crisis-response.com

Chief Scientific Editor
Ian Portelli, PhD, BCDM
ian@crisis-response.com

Sales & Marketing Director
Kirsty McKinlay-Stewart
kirsty@crisis-response.com

Global Operations Director
David Stewart
david @crisis-response.com

Design & Production
Chris Pettican
chris@crisis-response.com

Subscriptions & Administration
Thomas Morgan
subs@crisis-response.com

Subscriptions
Crisis Response Journal is published quarterly; it is available by subscription in hard copy, digital and online
subs@crisis-response.com

Back issues
Subscribers £25 (US\$30; €30) for hard copy edition (online editions free for subscribers). Non subscribers £40 (US\$51; €47)
backissues@crisis-response.com

Published by Crisis Management Limited, Sondes Place Farm, Westcott Road, Dorking RH4 3EB, UK
COPYRIGHT Crisis Management Limited 2017.
Articles published may not be reproduced in any form without prior written permission.
Printed in England by Henry Stone, Banbury, UK
ISSN 1745-8633

www.crisis-response.com

[join the CRJ LinkedIn group](#)

[follow us on twitter @editorialcrj](#)



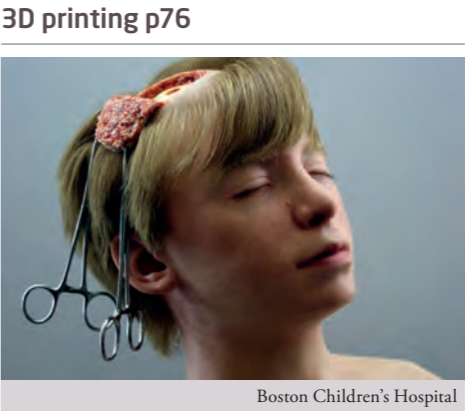
contents

News	4	The Grenfell Tower tragedy	28
Comment		The Grenfell Tower fire is an indication of the fragility of the crisis management frameworks upon which we so heavily rely, according to David Rubens	
The fickle finger of fake	8	Ransomware: The trap within the trap	30
Rob Shimmin examines the phenomenon of fake news and its role in crisis creation and management – how do we quieten the echo chamber?		Very few of us know when an attacker owns our computer with malware, and that’s the real problem, writes Todd Rosenblum	
Vehicles as terrorist weapons	12	Getting to grips with cyber security	32
David Stewart was Silver Command during the Glasgow Airport terrorist attack ten years ago. Here, he outlines how security measures have since deterred attacks using vehicles at airports		There are fairly straightforward things your business can do to help avoid being a victim of ransomware or other cyber crime, says Gary Fairley	
Terrorism & Security		Emergency management	
Disrupting the path of least resistance	14	What does resilience mean in the UK?	34
Since our last edition, there have been many high-profile terrorist attacks, says Roger Gomm. How can businesses, communities and governments improve their preparedness?		Sarah Ponesch interviewed five UK stakeholders with the aim of identifying the UK-specificity of resilience as a ‘culture’ in an ever-changing world	
Radicalisation in Central Asia	16	Organisational resilience	40
Radicalised operatives from the ex-Soviet Union regions of Central Asia and the Russian Caucasus are increasingly carrying out attacks elsewhere, says Lina Kolesnikova		Anticipation, assessment, prevention, preparation, response and recovery – these are the vital areas that any organisation should be looking at when considering its resilience, says Roger Gomm	
Lessons from the Lindt Café siege	18	Alternative community crisis paradigm ...	42
Editorial Advisory Panel Member Andrew Brown, who served as an expert witness into the siege inquiry in Australia, provides an insight into some of the findings of the final report on the incident, which resulted in several fatalities		Dennis Davis suggests that resilience should become more focused upon the citizen, with matters of vulnerability and consequence being considered at the planning stage	
Explosive threat mitigation in Iraq	22	Workplace violence crises	48
Major General Jonathan Shaw describes the scale of the explosive threat (ET) problems faced in Iraq, saying that mitigation is a vital precursor to stabilisation and reconstruction		Richard Diston examines workplace violence, saying that it can often be an organisational crisis. But how to eliminate violent conduct and ensure a safe workplace for all employees? The starting point is leadership	
Treating Afghanistan’s victims of war	26	Emergency management on islands	50
Emily Hough speaks to Dejan Panic, of the Emergency Surgical Centre, which treats victims of war and landmines for the whole of Afghanistan		How do you undertake disaster management on one of the world’s most remote islands? Ian Johnson describes the particular challenges of protecting the island of St Helena in the South Atlantic	



Cover story: Space technology for humanitarian and disaster applications
Cover illustration: Elisanth | Alamy

Ground search and rescue	54	R&D/Technology	
Martin Boyle speaks to Chris Boyer of the US-based National Association for Search and Rescue (Nasar)		3D printing in healthcare	76
Artificial Intelligence		3D printing has become a versatile and progressively cost-effective technology, permeating a variety of fields, say our R&D writers, led by Ian Portelli	
Leveraging AI for good	56	Drones for emergencies	78
AI has enormous potential for social good, says Houlin Zhao of the ITU, but we need paths forward for safe, trusted, ethical solutions		Petros Kremonas of EENA says that perhaps, in a few years, having drones available within an emergency rescue organisation will be as routine as having a telephone line	
Shaping Artificial Intelligence’s future	58	Computer modelling in large incidents	80
How we instill ethical principles during AI’s infancy could have positive or negative repercussions for decades, if not centuries. Emily Hough talks to Sherif Elsayed-Ali of Amnesty International to find out more		Friedrich Steinhäusler examines how 3D modelling of people, vehicles, weapons, explosions and the release of toxic materials can help first responders	
Space technology		In Depth	
We are the Space Race	60	What is the impact NIMS?	84
Laurence Marzell says the 1950s Space Race still pays dividends today, as we rely on information from space for services to keep us safe, secure and resilient		Nicholas B Hambridge, Arnold M Howitt and David W Giles examine how successful the diffusion of the National Incident Command System has been across the US	
A view from above: Earth observation	64	Robotics for Good: Part III	86
Dalia Kirschbaum and colleagues outline how NASA, working with partners, is helping to harness the scope and range of Earth observations for disaster response and risk reduction teams on the ground		Andrew Schroeder says that social automation is an issue of what kinds of conjoined human and technological systems are most likely to produce the ethical outcomes that we are able to agree on	
Space and the Sendai Framework	68	Firefighting in tunnels: Part IV	88
Space-based technology and Earth observation help in disaster risk reduction, say Joachim Post, Juan-Carlos Villagran and Luc St Pierre. But more effort is needed to make this data usable by developing countries		Christian Brauner discusses the limits of respiratory protection in underground transport systems	
Governance and ICT solutions	72	Early warning on small islands: Part II	91
Davide Miozzo and Davide Poletto describe some projects that aim to embed ICT and space technology in the daily work of first responders		Marlon Clarke and Danielle Evanson examine how vulnerability and capacity assessments are such a vital part of the process to enhance understanding of risks and reducing vulnerability	
The threat of orbital debris	74	Regulars	
Humanity relies on space technology, but this could stall if the issue of space junk is not addressed. Emily Hough speaks to Nobu Okada of Astroscale, which aims to secure long-term space flight safety		Events	94
		Looking back	97
		Frontline	98



comment

Few places have been safe from the reach of the vicious tendrils of terrorism in the short time since our last edition was published. We have seen attacks involving major loss of life in Pakistan, China, South Sudan, Libya, Iraq, Afghanistan, Nigeria, Egypt, Sweden, Russia and the UK. Sadly, this list is by no means exhaustive. We also witnessed the truly shocking pictures of people trapped in a high-rise tower in one of the world’s wealthiest capital cities (see p28 for Grenfell Tower analysis). On pages 30 and 32 we report on other human-caused crises, those of malware and cyber crime. Whether motivated by human malice or criminality, justified by ideological reasons, or exacerbated by poor or lackadaisical emergency planning, vulnerabilities and weaknesses are still repeatedly exposed. As *CRJ* and its authors have consistently stated over the years, the challenges presented by such incidents are dwarfed in terms of the possible human loss caused by climate disruption. And we have also examined what happens when security and climate issues collide. On the *CRJ* website, we noted recently how climate related issues can ripple out and trigger wider global security crises, as highlighted by a report that names 12 significant climate and security epicentres, all of which present extremely serious risks. As we go to press, Europe is in the grip of a heatwave dubbed ‘Lucifer’, and wildfires are raging in many parts of the world, while catastrophic flooding devastates other areas. Yet there is still profound resistance, lack of engagement or willful detachment – whether politically, economically, or institutionally – to acknowledge the potential impact of climate risks. How to embed resilience, prevention and mitigation in an effective and meaningful way, so as to engage governments, businesses, communities and individuals? A vital first step has to be discarding some of the entrenched and unproductive institutional or organisational terminology, definitions and doctrines that many organisations seem to adhere to so doggedly. Interminable pontification about pointless semantics and pushing narrow, short-term, self-interested motivations are simply dodging pressing crisis issues. It is time to set agendas aside and truly think in global human terms, eschewing treacherous tunnel vision and joining up the dots – we need to see the whole picture for it really is.

Emily Hough



What is the impact of the

Nicholas B Hambridge, Arnold M Howitt, and David W Giles gauge the diffusion of the National Incident Management System across the United States

As a consequence of the September 11, 2001, terrorist attacks, the US *Homeland Security Act* of 2002 mandated the creation of the National Incident Management System (NIMS) to be the standard method for managing emergency response operations at all levels of government regardless of incident type, size, or complexity.

The underlying logic of developing and deploying an emergency response system like NIMS/Incident Command System (ICS) rests on the need for co-ordination of resources, particularly in major events. Ideally, a robust emergency response, especially when involving multiple organisations and jurisdictions, requires effective collaboration so response tasks can be carried out with necessary urgency, maximum feasible effectiveness and cost-effectiveness, with minimal duplication of effort or unmet response needs.

The Congressional mandate for NIMS, however, did not in itself ensure success in diffusing NIMS practices broadly, let alone universally. The US has more than 89,000 units of subnational government – states, counties,

municipalities, school districts, and special districts. To achieve the potential benefits of a standardised emergency management system that fosters effective co-ordination, NIMS has to be diffused across levels of government and jurisdictions, be accepted by diverse professions, take root in hundreds of thousands of individual agencies and organisations, and spread through the public, private, and non-profit sectors.

Unlike many other kinds of innovation, responsibility for NIMS cannot be assigned to a special organisational unit in each of these entities; rather it requires full engagement by all agency personnel at the operating level (see Arnold M Howitt and Herman B Leonard, *A Command System for all Agencies?* *CRJ* 1:2, 2005). The broad sweep and depth of the NIMS requirement entails a massive implementation process – one that is still going on 15 years after the Congressional mandate.

The ICS is fundamental to NIMS as a framework for managing operations at or near the scene of an emergency. It provides responders with a way to co-ordinate emergency efforts through a common, flexible, and scalable command structure that organises response under an incident commander and a sub-organisation of four major sections: Operations; planning; logistics; and finance/administration.

As the scale of response expands, responders may organise sub-units of the four core sections, either by functional specialisation (eg fire

suppression operations group and emergency medical operations group) or by geographic sector, called divisions. See Figure 1 for depiction of a basic ICS structure and an expanded structure for complex events.

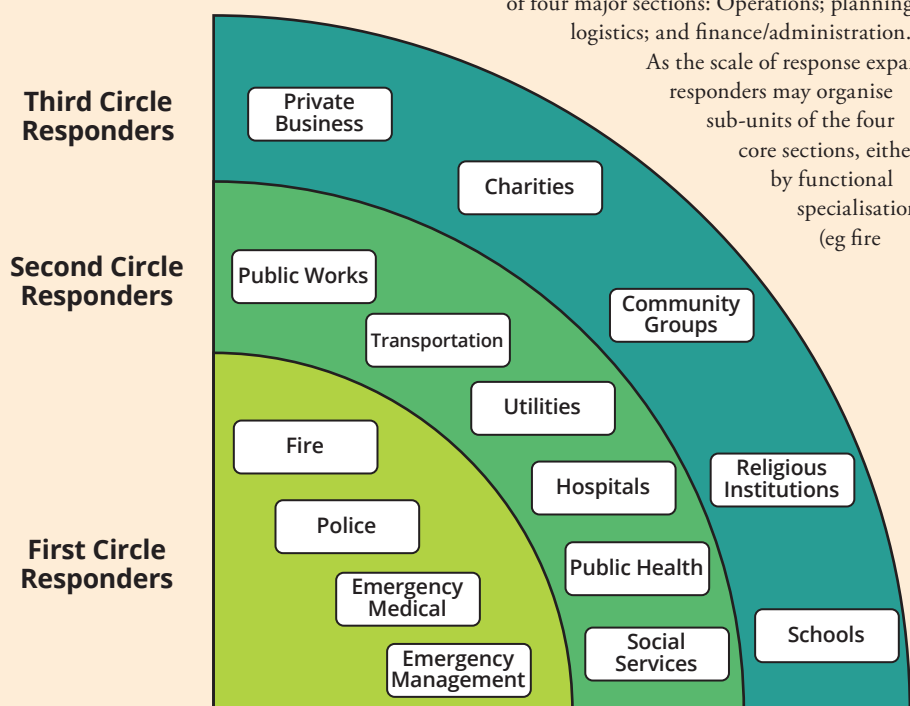
So what is the impact of the NIMS mandate? To ensure that ICS is used as universally as possible, the US federal government issued NIMS implementation requirements starting in the financial year 2005, which gave jurisdictions two years to comply with the full array of NIMS implementation standards. NIMS compliance was made a precondition for any agency or organisation to receive homeland security preparedness funding – a potentially powerful incentive for adopting and implementing the system.

However, the impact of actually withholding funds from jurisdictions that did not comply with the NIMS mandate proved too strong or even counter-productive to those developing the regulations for NIMS compliance. Withholding funds would have removed resources that those entities needed to improve emergency response systems, and that would undoubtedly have caused political reaction by local, state, and federal officeholders representing those jurisdictions. Therefore, states and sub-state jurisdictions, when applying for homeland security grants, have only been asked to self-certify, with minimal documentation, that they are NIMS compliant.

Although it has only lightly enforced NIMS compliance, FEMA has fostered NIMS implementation by issuing guidance documents to all levels of government, as well as to private industry and non-profit organisations. In addition, FEMA has created NIMS training resources for specific disciplines, including transportation, healthcare, hospitals, higher education, schools, public works, public health, and volunteer organisations. FEMA's attention to the variation among emergency response groups has been important to the implementation process because it makes a seemingly monolithic system adaptable to the variety of cultures, missions, needs, and capabilities across emergency response disciplines.

Understanding the differences among professions that participate in emergency response, particularly the contrast between first responders and other disciplines, is critical to evaluating the success of NIMS implementation thus far and improving it's moving forward.

The term 'first responder' in US legislation means: "Federal, state, and local governmental and non governmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities)...." But other public and



NIMS mandate?

non-public agencies may become crucial actors in emergencies. This can be illustrated by the imagery of concentric circles where the inner circle is occupied by agencies whose principal mission is emergency management and the outer circles contain all the other organisations with potential involvement in emergency-related activities but which do not consider emergency management their core mission (Figure 2 opposite page).

Research has consistently identified several factors as having an impact on NIMS implementation – and on emergency preparedness in general. But these factors may work less effectively for organisations in the outer circles than for first responders.

The first factor is compliance requirements and enforcement. Federal preparedness funding for states and localities was made contingent upon NIMS compliance, although FEMA has required only state-level self-certification. While federal grant funding could be a strong incentive to compel NIMS compliance for first response organisations, many second and third circle responder groups – for example, private industry and NGOs – do not rely on this funding.

Comprehension of risk is another factor. An organisation's or individual's level of perceived risk of experiencing a severe emergency influences their preparedness. When the level of perceived risk is low, the chances of a person or group doing something to prepare for or mitigate that risk are also low. Conversely, when persons or groups believe that a risk is likely to affect them, they are more likely to take action to prevent or prepare for it. Therefore, helping organisations in the outer circles to understand their risks is a primary step. The federal government has begun to put greater emphasis on risk assessments as part of the National Preparedness Goal and National Preparedness System.

Commitment of resources is a critical element. For second and third circle organisations, diverting resources (time, money, and staff) away from their own mission-critical activities and into emergency management programmes has proved problematic, especially when budgets are shrinking or they have limited financial and administrative resources. The commitment of executive leadership within these organisations to fund and support emergency planning and preparedness initiatives is therefore very

important for NIMS implementation.

Furthermore, outer circle organisations may perceive NIMS/ICS as overly prescriptive and rigid and hence unsuitable for those that do not primarily function as command and control hierarchies. Some have argued for flexibility in customising NIMS in ways relevant to each individual organisation's needs, structure, and culture, while maintaining sufficient fidelity to the basic system so that collaboration with other organisations remains feasible.

Collaboration with other responders is another important factor. A number of observers cite the benefits of pre-incident collaboration between emergency response groups, whether in planning, training, or exercising. Second and third circle groups that are able to maintain close linkages to first response agencies are more likely to be successful in emergency planning and NIMS implementation efforts.

And finally, we have the issue of consistency of use. Infrequent utilisation of NIMS is another obstacle to full implementation, particularly by outer circle responders. While first responders usually have opportunities to use NIMS/ICS as part of their normal work activities, second and third circle responders encounter emergency situations much less frequently and are therefore

more likely to be uncomfortable using NIMS when they do respond to emergencies.

To what extent therefore is NIMS being implemented effectively in second and third circle organizations? Part 2 will explore that question in the context of transit and highway agencies. **CRJ**

■ A longer version of the research reported here appears in *Co-ordination in Crises: Implementation of the National Incident Management System by Surface Transportation Agencies*, Homeland Security Affairs 13, (March 2017); www.hsaj.org. Development of this article was supported by the New England University Transportation Center with funds from the US Department of Transportation's University Transportation Centers programme. Additional support was provided by the Ash Center for Democratic Governance and Innovation, the Taubman Center for State and Local Government, and the Program on Crisis Leadership – all of the John F Kennedy School of Government at Harvard University

Authors

NICHOLAS B HAMBRIDGE is Associate Director of Risk & Compliance Services at Harvard University and previously served as Harvard's Associate Director of Emergency Management, where he oversaw the University's emergency planning, preparedness, response, and recovery activities.

ARNOLD M HOWITT is Faculty Co-Director of the Programme on Crisis Leadership (PCL) and Senior Adviser of the Ash Center for Democratic Governance and Innovation, both at the John F Kennedy School of Government, Harvard University. He is a Member of CRJ's Editorial Advisory Panel.

DAVID W. GILES is the Associate Director and Senior Research Associate of the Program on Crisis Leadership at the John F Kennedy School of Government, Harvard University

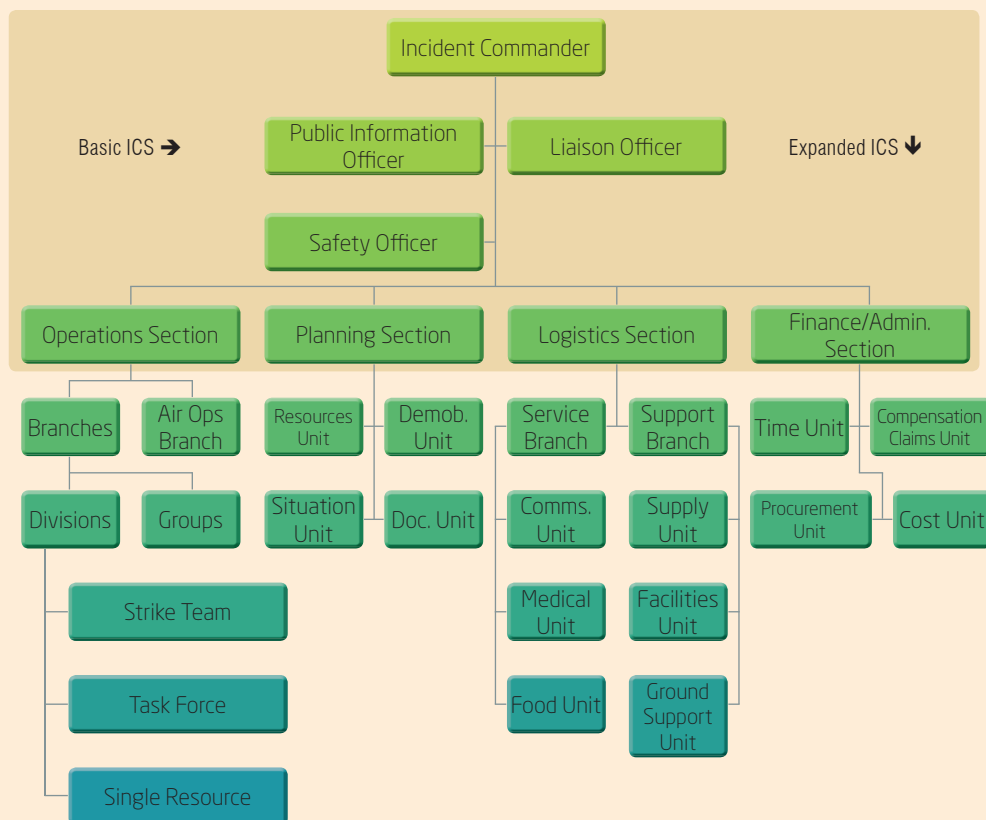


Figure 1 (right): Basic ICS structure and expanded ICS structure for complex events; Figure 2 (left): Other crucial actors in emergencies

Adapted from FEMA ICS for Single Resources and Initial Action Incidents; emilms.fema.gov/IS200b/ICS01summary.html

CRISIS▶RESPONSE

www.crisis-response.com JOURNAL

PROTECTION | PREVENTION | PREPAREDNESS | RESPONSE | RESILIENCE | RECOVERY



SUBSCRIBE NOW

You know you want to!

Authoritative global coverage of all aspects of security, risk, crisis management, humanitarian response, business continuity planning, resilience, management, leadership, technology and emerging trends

PRINT | ONLINE | DIGITAL |