

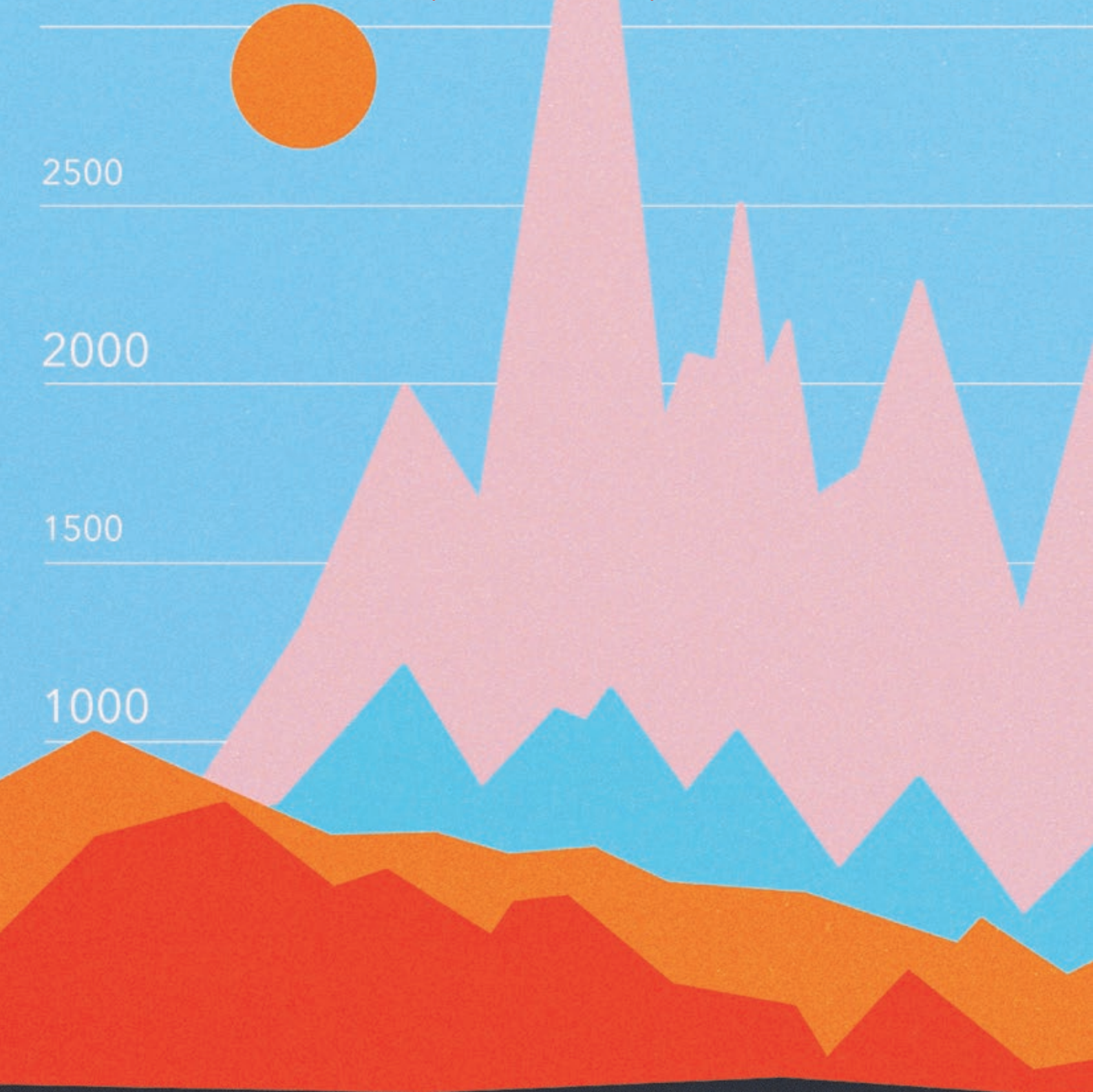
# CRISIS ▶ RESPONSE

VOL:15 | ISSUE:2 | JUNE 2020

WWW.CRISIS-RESPONSE.COM

JOURNAL

Protection Prevention Preparedness Response Resilience Recovery



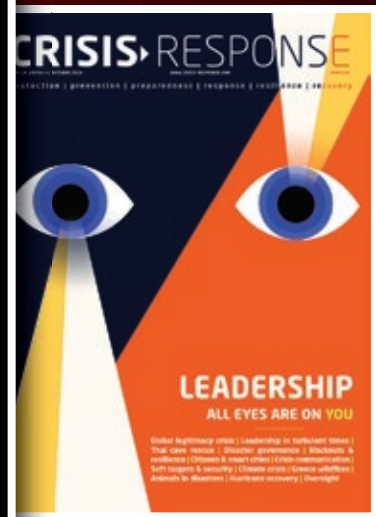
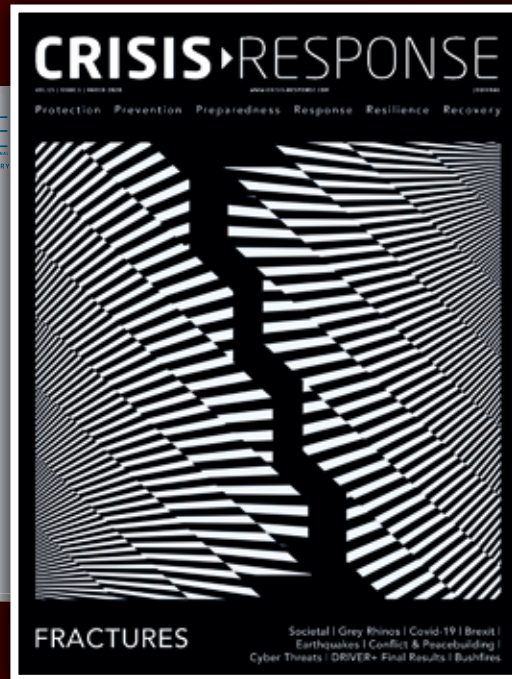
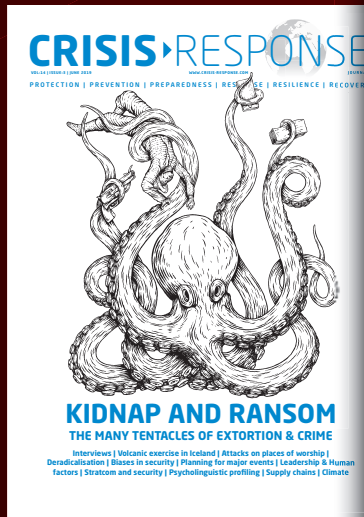
## COVID-19

Emergency Management | Mental Health | Supply Chains | Economy | Business Continuity | Science on the Front Line | Attacks on First Responders | Climate

# CRISIS ▶ RESPONSE

JOURNAL

PROTECTION | PREVENTION | PREPAREDNESS | RESPONSE | RESILIENCE | RECOVERY



## SUBSCRIBE NOW

visit [www.crisis-response.com](http://www.crisis-response.com) for rates and special offers



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

# contents

## Editor in Chief

Emily Hough  
emily@crisis-response.com

## Editorial Assistant

Claire Sanders  
claire@crisis-response.com

## Projects Development Manager

Derya Kemmis  
derya@crisis-response.com

## Design & Production

Chris Pettican  
chris@layoutdesigner.co.uk

## News and Blog research

Lina Kolesnikova  
lina@crisis-response.com

## Web Support

Neil Moultrie


## Subscriptions

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


Published by Crisis Management Limited, Sondes Place Farm, Westcott Road, Dorking RH4 3EB, UK  
COPYRIGHT Crisis Management Limited 2020.

Articles published may not be reproduced in any form without prior written permission.

Printed in England by The Manson Group, UK  
ISSN 1745-8633

 [www.crisis-response.com](http://www.crisis-response.com)

 join the *CRJ* LinkedIn group

 follow us on twitter @editorialcrj



<b>News</b> .....	<b>4</b>	<b>Supply chain surge capacity</b> .....	<b>36</b>
<b>Comment</b>			
<b>Time to stand up and be heard</b> .....	<b>8</b>	Covid-19 saw the entire world simultaneously in need of the same lifesaving tools. Bill Peterson explores how globalisation, interconnectedness and the constant quest to drive prices down in the public and private sectors have led to a battle between national and international interests	
Eric J Russell asks why warnings and advice from disaster managers and experts go unheeded with such depressing regularity			
<b>Disaster management and Godzilla</b> .....	<b>12</b>	<b>Lockdown exits and supply chains</b> .....	<b>38</b>
<i>Shin Godzilla</i> is the metaphorical embodiment of contemporary and institutional disaster management in a large-scale catastrophe, say experts from the University of Alaska Fairbanks			
<b>Climate change in the time of Covid-19</b> ...	<b>16</b>	<b>Science on the front line</b> .....	<b>42</b>
Alice C Hill and William Kakenmaster warn that we cannot divert focus from the crucial efforts needed to reduce emissions permanently			
<b>Covid-19 analysis</b>			
<b>Emergency management</b> .....	<b>20</b>	<b>Building equity in crises</b> .....	<b>46</b>
The pandemic is a make-or-break test of crisis response preparation and is likely to be the first of many global crises. We shouldn't just be dealing with this one, but preparing for the next, says John Drake			
<b>Why have an independent inquiry?</b> .....	<b>22</b>	Covid-19 disproportionately affects people of colour and those living with poverty and medical fragility. Marcus Tillman Coleman Jr calls for change	
Lucian J Hudson presents the case for a timely, independent lessons learned inquiry in the UK, calling for a new social contract that requires national threats to be reviewed regularly and visibly			
<b>Is there really a 'new normal'?</b> .....	<b>26</b>	<b>The psychosocial burdens of Covid-19</b> ....	<b>50</b>
Citizens in Western Europe, North America and beyond have never had restrictions on our freedom such as those mandated by the response to Covid-19, writes Lyndon Bird. What does this bode for the future?			
<b>No one is coming</b> .....	<b>30</b>	Virtually everyone across the globe will experience varying degrees of psychosocial burden as a result of this crisis, write Gregory Ciottone, Todd Benham, and colleagues	
Emergency managers will still be working in communities to pick up the pieces long after the Covid-19 crisis is over. Sherry-Lea Bloodworth Botoj says this is nothing new and that the recovery process often lacks the necessary support			
<b>Overcoming mental health challenges</b> .....			
There are many effects of the pandemic that are deleterious to our wellbeing. What can we do to keep ourselves healthy, both physically and mentally? Lyzi G Cota provides some answers			
<b>Drawing from hostage experiences</b> .....			
Sue Williams advises on how to cope with isolation, whether in lockdown or a prolonged hostage situation, using 'conduct after capture' techniques			
<b>Harnessing AI:</b> .....			
Artificial intelligence told us about the pandemic before the WHO knew about it, writes Stephane Martin			

## Societal disaster management p12



Gracie Broom

## Supply chain surges p36



Gracie Broom



## comment

Cover story: Covid-19: A snapshot of fatality rates March 31 – May 9, 2020 (USA, UK, Italy, Spain, South Korea)

Cover image: Gracie Broom

<b>Transformational technology</b> ..... 60	<b>Tackling right-wing lone actors</b> ..... 81
Susan Morgan asks us to question the long-term implications of deploying digital technology as a response to Covid-19	We must hold a mature debate on home-grown terrorism and its causes, but society, governments and industry are turning a blind eye, says Florian Hartleb
<b>Infecting the truth</b> ..... 63	<b>Response</b>
At a time when trust between government and the population is vital, Covid-19 presents a chance for fake news, disinformation and conspiracy theories to abound, reports Ørjan Karlsson	<b>Superyachts in island disaster response</b> .. 84
<b>Communication and recovery</b> ..... 64	There is significant potential for superyachts to have an impact in island-based responses, say Grant Dawson and Michael Court
Exercises and training focus on responding to a crisis quickly, but they rarely consider how to deal with the situation that follows, writes Amanda Coleman	<b>Online learning in lockdown</b> ..... 86
<b>A humanitarian perspective</b> ..... 66	Anne Garçon contends that the need for local humanitarian action is greater than ever and the demand for easily accessible online learning is growing as people adjust to new ways of life
Andrew B Brown looks at how a faith-based INGO has kept its staff safe while helping to protect vulnerable communities	<b>The future of emergency services</b> ..... 88
<b>Healthcare</b>	Next Generation 112 incorporates new technologies to revolutionise the work of emergency services, reports Beatriz Peon
<b>Delivering care in complex disasters</b> ..... 68	<b>The critical communications agenda</b> ..... 90
Planning a medical response must go beyond the immediate to address the long-term health care needs of affected communities, says Ayman S Jundi	Mladen Vratonjić describes the work of the Critical Communications Association, which works to advance the quality of wireless communications
<b>Shifting the balance in medicine</b> ..... 70	<b>Drones and humanitarian missions</b> ..... 92
Margaret Heffernan used to object to the idea of telemedicine because she thought it was less human and a denial of comfort in times of need. But, she says, she has changed her mind	Drones can enhance the safety of citizens and responders and increase operational effectiveness. They are an essential part of the public safety response toolbox, according to Charles Werner
<b>EMS workers in hostile environments</b> ..... 74	<b>The drone threat landscape</b> ..... 94
Emergency Medical Service workers are exposed to aggression and violence in their daily operations, but they are not always prepared. A change in mindset is required, contends Christoph Lippay	Drones can bring innumerable benefits, but this could come at a price. Andrew Staniforth looks at the development of rules and systems to govern their use
<b>Violence &amp; extremism</b>	<b>Regulars</b>
<b>Can we prepare for school shootings?</b> ..... 78	<b>Events</b> ..... 96
Attacks on students continue to happen sporadically throughout the world. Kjell Brataas takes a closer look at lessons learned	<b>Frontline</b> ..... 98
	Claire Sanders speaks to Chris Sheldrick, CEO and Founder of what3words, to find out how businesses and emergency services make use of its technology

**C**risis have a way of exacerbating underlying vulnerabilities. Once the protective surface has been flayed from society, its pre-existing conditions are exposed and rendered more acute.



Authors in this edition warn how Covid-19 lays bare inequity, inequality and poverty; the virus is not indiscriminate. And when ingrained injustices reach a peak, righteous anger and frustration inevitably spill over into discord, presenting an opening for those who seek to profit from inflaming societal division.

The Covid-19 crisis – which has taken so many lives and wreaked such misery, fear and pain – raises questions about humanity's ability to work together against common, global threats. With a few notable exceptions, the virus seems to have caught governments on the back foot, illustrated by a failure to understand the full cascading consequences and potential systemic nature of a pandemic.

Perhaps the first mistake of many was an initial inclination to treat this as a 'health' emergency, failing to appreciate how interdependencies allow the virus to rampage across all layers of a society – from individuals and communities, to livelihoods, businesses, economies and supply chains – calling our very values and global models of co-operation into question.

Another glaring omission is evident – where is resilience? Why is the voice of emergency management unheeded by so many at the top levels of governance and the public alike? On p8, Eric Russell attempts to find answers, while on p42 Paolo Garonna explores how science and its global institutions have been devalued and exploited – to the extent of making them viewed as irrelevant in some quarters.

How are we going to cope when larger, more interconnected and destructive crises sweep our way? The answer must not lie in retreating into conflict and hostility. But we cannot come out of this as we were before, and this may be a good thing, as Marcus Coleman notes on p46. We can transform tragedy into opportunity for all. We can examine our global institutions, empowering them to act with authority and universal legitimacy, while maintaining vigilant oversight. We can place our resilience experts where they should be – trusted, experienced voices, whose knowledge is valued and respected at the very highest levels.

The alternative is to retreat into narrow, nationalistic opportunism, privilege and self-interest, sticking tiny plasters on the exposed, weeping wounds of our global society.

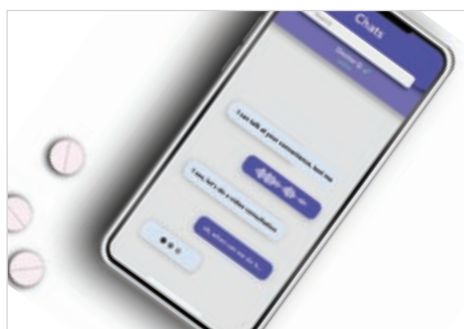
Surely we can do better than this?

### Science on the front line p42



Thomas Kuhlenbeck | Ikon Images

### Telemedicine innovation p70



Gracie Broom

# Disruptive technology: The drone threat landscape

Drones have democratised the skies and brought innumerable benefits to first responders and disaster management agencies alike. Unfortunately, in the wrong hands, they have the capacity to damage, destroy and disrupt. **Andrew Staniforth** looks at the development of rules and systems to govern their use



Commercial drones have earned their status as a contemporary disruptive technology, proving themselves to be an innovative development that has significantly altered the way that consumers, industries and businesses across the world operate.

Drones have become an increasingly familiar aspect of modern life and work, playing a growing role for emergency services in their response to crisis. But the

sudden and dramatic rise of the use of commercial drones from hobby-enthusiasts to a ubiquitous business tool remains in its infancy, and governments are struggling to find effective ways to address the full range of safety and security concerns associated with the drone revolution.

During a time when all organisations and governments across the world are under pressure to be more efficient, environmentally friendly, innovative and ambitious in how they deliver services, drones offer a lens onto the

world below. Gathering data quickly and accurately from places that are hard to reach, they can create a unique record in near real time. This can make a crucial difference in managing costs, controlling risks, increasing safety and influencing outcomes.

Drones are democratising the sky and enabling new participants in aviation, quickly evolving beyond their military origin to become powerful business tools. In the US, projected growth of the market for commercial drones is set to rise from \$850 million this year to \$1 billion in 2022. The largest share of the US drone market is expected to be across all government departments, predicted to reach a value of \$420 million over the next two years.

In the UK, the government's Counter-Unmanned Aircraft Strategy published last year, supported industry predictions that by 2030, 76,000 drones will be flying across UK skies, part of a projected drone technology industry with the potential to increase UK Gross Domestic Product (GDP) by £42 billion (or two per cent) over the next ten years.

The predicted rise in the US and the UK drone markets is also anticipated throughout European member states, as well as other nations across the globe. The future of flight is currently being dominated by



the proliferation of drone technology and all industry estimates provides strong evidence that drones are headed for new heights in the business world. But the rapid growth of the drone industry has so far outpaced the development of rules and systems to govern their use, resulting in a growing threat landscape that presents major public safety and national security concerns.

The rapid proliferation of drones represents a disruptive technological innovation that continues to develop at exponential speed, and on a global scale. Autonomously piloted systems have the potential to revolutionise how disasters and crisis are managed by first-responder agencies. At the same time, this new technology is being hijacked by those with hostile intentions, adopting and adapting the use of drones for their own nefarious purposes. Unfortunately, in the wrong hands, drones have the capacity to damage, destroy, disrupt and, when used as a terrorist tactic, have the capability to conduct deadly and determined attacks.

The increasing use of UAVs by amateur enthusiasts and professionally qualified drone pilots has resulted in a growing catalogue of incidents ranging in seriousness from minor occurrences causing public nuisance, to major threats to national security. The misuse of drones includes the intentional invasion of privacy upon individual citizens by persistent paparazzi, along with physical injury caused to pedestrians and damage to vehicles and property by enthusiasts recklessly ignoring regulations and losing control of their drones.

Such increasing misuse has also resulted in police officers in many nations across the world having to attend incidents and accidents involving drones and, more concerning, having to investigate a rise in crimes involving drones purchased online or direct from stores. These investigations have included allegations that drones are being used to supply illegal drugs into prisons, human traffickers are using them to monitor border patrols, paedophiles are hovering over children's playgrounds and burglars are scoping out people's properties.

Aviation facilities, particularly large airports, also remain attractive targets for drone pilots with hostile intent because of their high-profile and iconic nature. An attack or malicious and disruptive incursion using a drone, has already proven to have serious safety, security and economic consequences. Despite the knowledge of rogue-drone activity in restricted areas, and the clear and present danger posed to aircraft from potential drone-strikes, reports of rogue drone activity at airports across the world continue to occur with alarming regularity.

Aside from the targeting of airports and aircraft by rogue drone pilots, all manner of threats from increasingly sophisticated drones with larger payload capacities are set to provide greater challenges to public safety and national security, including the economic wellbeing of businesses across the world from a drone-enabled cyberattack.

As digital circuitry and wireless technology become an increasingly integral part of consumer and industrial goods, the opportunities available for cyber criminals to compromise or exploit these items grows. Drones are now an emerging cybersecurity concern – both as targets for cyberattack, and as potential attack vectors for malicious actors. Drones use the most advanced technological equipment and research into these vehicles

is providing continuous improvements, resulting in a new generation of drones characterised by high performance, high autonomy and extreme versatility, which make their use suitable for many applications.

The rapid proliferation of drones does not necessarily mean they are safe to use, as many have inherent and potentially serious design flaws. Given their manoeuvrability, small size, and the fact that their combination of on-board processing power, photographic equipment and connectivity makes them the equivalent of flying laptops, it is no wonder that drones are now perceived as viable threats to information security. Poorly secured or unsecured wireless networks are seen as particularly vulnerable, with attack scenarios envisaged where compromised or purpose-bought drones could be

## Drones are enabling new participants in aviation, rapidly evolving beyond their military origin to become powerful business tools

flown or discreetly landed in the vicinity of a hot spot, and used to stage cyberattacks over guest and short-range WiFi, Bluetooth, and other wireless connections.

Despite the new generation of drones being packed with the latest technical tools, a number of independent tests by researchers have demonstrated how high-end drones commonly deployed by government agencies, including police forces, can be remotely exploited by rogue hackers. Researchers have found security flaws in drones' radio connections, providing opportunities to exploit the lack of encryption between the drone and its controller module.

To facilitate attacks on drones, the discovery of the 'Maldrone' malware five years ago was a wake-up call to defence and security policymakers across the world. As a type of malware specifically intended to hack into drones via internet connections, Maldrone was used to either swipe the data that drones had collected, or to take over their physical control and direction.

### Expanding attack vectors

The hijacking of drones continues to present a danger within the ever expanding attack vectors of the contemporary cyber criminal. To mitigate the threat, it is essential to safeguard every single component of the increasingly sophisticated drone from cyberattack, a major industry challenge, as when drones were initially developed, cyberattacks were not considered high priority.

To reduce the risk further, in-depth research into cyberattack threats and vulnerability identification of drones is needed. This research should include the study of more sophisticated attack scenarios together with the development of metrics for drone cyberattacks. Conducting rigorous and collaborative programmes of drone cybersecurity research will serve to strengthen the safe use of drones and reduce their vulnerability to attack from contemporary cybercriminals.

#### Author



**ANDREW STANIFORTH**  
is Director of  
Saher-Europe and a  
Member of CRJ's Advisory Panel



# CRISIS ▶ RESPONSE

JOURNAL | WEBSITE | EVENTS | SOCIAL MEDIA | NETWORKING | BUSINESS DEVELOPMENT



## MULTIPLY

the force of your business

**Open doors** to the people you really want to meet. **Influence your market** and **build your brand awareness**, across the global crisis and emergency response fields.

### Key Network Partnership:

We call them Key Network Partnerships. Because you're not just becoming a partner of ours - but leveraging access to our entire global network. It's about connecting you with the right decision-makers. We open doors and introduce you to the right people, with the power to transform the next phase of your business development. And it's about intelligently marketing your business, to your target audience, across our global platforms. Extending your reach, increasing your exposure and driving your brand awareness.

**Call CRJ today** about becoming a Key Network Partner on **+44 (0)203 488 2654**

PROTECTION | PREVENTION | PREPAREDNESS | RESPONSE | RESILIENCE | RECOVERY

[www.crisis-response.com](http://www.crisis-response.com)



# Strategic Solutions for Global Issues

Our experienced multi-national team bring years of expertise in all aspects of Resilience, Crisis Management, Policing and Security services, making Crisis Management Limited a key resource for any level of related work, whether at a local, national or international level across public, private or voluntary sectors. We do not believe in 'off the shelf' solutions but seek to work with all clients to ensure bespoke services that meet clients' needs and expectations. No projects are too small or too large.

Our multi-disciplined team has vast experience across all sectors and continents. Our experts have the flexibility to provide support at State or Government level for long term work, as well as bespoke niche work on a smaller scale and for short periods. The can-do approach of our team means that we can provide support at short notice if required.

- > International Experience
- > Bespoke Service
- > Flexibility
- > Customer Focus
- > Communication Expertise
- > Breadth of experience

[www.crisismanagementlimited.com](http://www.crisismanagementlimited.com)

[info@crisismanagementlimited.com](mailto:info@crisismanagementlimited.com)



**CRISIS MANAGEMENT**  
LIMITED