

CRISIS *comm*

With the London Olympic Games only a year away, Tony Kingham analyses the latest technology which will provide emergency services with secure communications during a terrorist attack or national disaster

The first duty of any government is to provide security for its citizens. Historically that would mean threats from other nation states and some primitive law enforcement on the streets at home. Not much, if anything, would or could have been done to protect the population against natural disasters like flood, famine or disease; these would simply be seen as "acts of god" and beyond the writ of man to do anything but endure. Even as recently as 1918-19, an influenza pandemic killed an estimated 20-40 million people which is more than the total casualties in the First World War and more deadly than the bubonic plague.

Today science, technology, medicine and communications have changed our understanding and view of the world and, as a result, what we expect from our governments. We now expect governments to protect us from any hazard from this world and beyond it. Natural disasters pose the greatest threat to life and property, and the world seems to have experienced plenty of those in recent years including earthquakes, tsunamis, floods, storms, pandemics and volcanic ash clouds.

Then, of course, there are the more remote possibilities of major global disasters like a meteor strike, such as the so called Tunguska event in Russia in 1908 that caused an explosion that knocked over an estimated 80 million trees covering 2,150 square kilometres. Or maybe a super volcano like Yellowstone, which scientists have revealed has been on a regular eruption cycle of 600,000 years. The last eruption was 640,000 years ago... so the next is overdue.

Although the threat of conventional war in the developed world has receded, though not disappeared, other threats have emerged as a result of advanced technology. Rogue states and global terrorists, while not a modern invention, now have the ability to deliver far more devastating blows to our society through the use of modern inventions like dirty bombs, chemical attacks, cyber attacks, WMD and so on.

Industrial disasters such as the those at Bhopal in India, Chernobyl in Russia and the ongoing nuclear disaster in Fukushima, which is still being played out as this article goes to press, are all obvious examples of unexpected home grown disaster that can strike us at any time.

Whatever the threat or disaster, it is the ability of



©Paradigm Secure Communications

Communications



the authorities to organise and move the available resources to the point of most need that is the key to managing the disaster effectively. Whether it is for search and rescue, medical assistance, shelter, sustenance or law and order, fundamental to the principle of good organisation is good reliable and resilient communications.

This lesson was clearly demonstrated during the recent riots on the streets of British cities. It was only after the police were able to mobilise and concentrate resources from across the country to the crisis points that the situation was brought under control. The riots also demonstrated that, even in a highly developed and prosperous society like the UK, and in the absence of an ongoing national disaster, there are always criminal and delinquent elements that pose an opportunistic threat to the vast majority of their law abiding fellow citizens. It is therefore not difficult to imagine the sort of anarchy that could reign in the streets should some sort of disaster hit the UK.

Good communications are taken for granted and we are increasingly dependent on them for the necessities of life – from earning a living to the weekly shopping delivery. Most of those communications are being relayed over the existing Public Switched Telephone System (PSTN) infrastructure. Quite apart from all landline telephone calls, virtually all computer information is already relayed via the PSTN, and the proliferation of technologies like Voice over Internet Protocol (VoIP) as a first choice for individuals and businesses will only increase our dependence on the existing infrastructure. According to a recent Ofcom report mobile data traffic has increased 40-fold in three years, but even this will be running over the PSTN backbone at some point.

According to Tom Swarbrigg, HITS Project Manager within the Resilient Communications Programme of the UK's Civil Contingencies Secretariat: "Few communications systems are completely reliable or resilient. They rely on multiple interconnections and dependencies which are not well understood and there are often unidentified points of failure.

"Key communication lines tend to follow other infrastructure, such as bridges, rails, roads, canal and sewers. Therefore something as simple as a single bridge collapse during flooding can cause major local communications problems." In the event of a national disaster, although a complete national failure of the telecommunications system is unlikely, local communications failure or serious degradation of service within the disaster area is probable, due to damage to infrastructure, loss of power or simple overload. Mobile systems are particularly vulnerable to this.

To guard against this eventuality and ensure that the UK Government and emergency services are able to effectively respond to the situation, the UK has

CRISIS COMMUNICATIONS

developed the High Integrity Telecommunications System (HITS). HITS was developed by the UK Government's Civil Contingencies Secretariat (CCS) in a partnership with Paradigm Secure Communications and the UK Ministry of Defence (MOD). The CCS is part of the UK Government's Cabinet Office and works across government and industry to improve the ability of the UK to respond to and recover from significant emergency events.

Paradigm is the prime contractor for the Skynet 5 contract with the UK Ministry of Defence. This programme provides all secure voice, data, video, Internet and broadcast communications for UK armed forces operating anywhere overseas. They also provide secure communications for other Nato member nations, including the US military. They own and operate seven military-hardened satellites that are resistant to any known attack and have both onboard and ground-based technology to overcome the interference threat posed by high solar flare activity.

HITS is a secure and resilient satellite-based communication system capable of delivering secure data and telecommunications completely independently from the main UK telephone network. The system is designed to provide telephone and Internet communications to the emergency services and related agencies in the event of a national emergency, when the existing landline or mobile networks are either down or seriously degraded. It is, however, completely interoperable with those parts of the regular networks that are still functioning, and so will facilitate the break-out of calls onto other networks such as mobile phones.

The system is funded by central government and made available free to any emergency services in England and Wales. It is installed at the Central Government Crisis Management Facilities, COBR, and at each of the UK's Devolved Administrations Crisis Management Centres. It is deployed at fixed sites across the UK, mainly in police Strategic Command Centres (SCCs) because the police usually the lead service in times of emergency. Every HITS installation comes with a number of phones and laptops – usually three of each – as well as at least one networked printer.

In addition to the core network sites, each police force area will also have at least one pre-determined fallback location, where HITS Transportable Terminals can be deployed. These fallback locations are designed as an extra level of communication security should any of the main HITS installations be perhaps within in the disaster area and so be unavailable as a result.

The system has been designed to fully inter-operate with the already existing National Resilience Extranet (NRE). This is the system that provides the UK resilience community with a common system, accessible via the internet for efficient and secure communication and exchange of information – allowing users to work together on routine planning, share best practice, and store documentation for others to access, so if the regular network is down, the NRE will still be available.



©Paradigm Secure Communications

Industrial disasters like the Buncefield explosion (above) and terrorist attacks have revealed the need for effective and secure emergency communication channels

Tony Kingham is a journalist, publisher and PR consultant, specialising in the defence and security markets for more than 25 years. He is the Communication Director of BORDERPOL and publisher of www.WorldSecurity-index.com.

HITS also includes the three transportable terminals mentioned earlier. These can be deployed anywhere in England and Wales and will usually be driven to the relevant location, although they can be carried by whatever transport is available. They are on call 24/7 and can be on the road within six hours of an emergency call out by the Cabinet Office.

Each transportable unit comes with up to ten digital phones and laptops, so they can effectively act as a mobile command centre wherever it is needed. They are equipped with their own generators and fuel, so are able to operate fully autonomously for up to seven days. Each of them has trained Paradigm personnel on hand to support the emergency services throughout the deployment.

The Cabinet Office have been able to test the system regularly by deployments of the transportable terminals at key events where regular mobile communications coverage are patchy due to the remoteness of the location or where the conventional telecommunications are under extreme pressure. These have included sporting events in the lead up to the London 2012 Olympic Games, national counter-terrorism exercises and the recent visit to the UK of the Pope.

HITS has to date been considered so successful that the Cabinet Office is exploring options to expand the system beyond the core network, as well as developing the existing capabilities further. This might include central government business continuity sites, as well as some specialised national response centres. Watch this space!



ORDER YOUR SUBSCRIPTION TODAY!

2011 SUBSCRIPTION RATES

	1 Year 10 issues	2 Years 20 issues	3 Years 30 issues
UK/Europe	£125/€140	£215/€230	£280/€300
USA/Canada	US\$285	US\$430	US\$560
Rest of World	£180	£270	£330

SUBSCRIBE ONLINE: www.intersec.co.uk

Or complete and return the form below:

Please reserve **intersec** now, and send it to me at the address below for: 1 year 2 years 3 years (Please tick)

I enclose a cheque for the sum of _____ payable to "Albany Media Ltd"

Or:

Please debit my VISA / MASTERCARD / DELTA / MAESTRO

(Please delete as applicable)

Card No:

(Please note that all American/Canadian card payments will be charged at the sterling equivalent)

Expiry Date: _____ Issue No: _____

Signed: _____ Date: _____

I would like to automatically renew my subscription on expiry. Please notify me and automatically debit my card unless instructed otherwise

If you wish to subscribe, but your accounting systems require an invoice, please tick here, complete the rest of the form and send it to us for immediate action.

Please send me an invoice

SUBSCRIBER DETAILS	
Name:	_____
Job Title:	_____
Organisation:	_____
Address:	_____ _____ _____
Country:	_____ Zip/Post Code: _____
Email:	_____
Phone:	_____
If you do <u>not</u> wish to receive information from us in the future, please tick the boxes below:	
<input type="checkbox"/>	I do not wish to receive other offers from intersec (eg: our events/shows)
<input type="checkbox"/>	I do not wish to receive information & special offers from other carefully selected companies

intersec – The world’s leading Journal of International Security is published 10 times a year. With current analytical features from a top team of contributors and in-house specialists, backed by international news pages, **intersec** is essential reading for those who take security and law enforcement seriously.

Please complete this form and return it with your remittance for the required period to the address shown below.

Subscription rates covering two and three year periods offer a valuable discount as well as enabling you to beat inevitable price rises.

TYPE OF ORGANISATION
(Please tick a maximum of two boxes)
A1 <input type="checkbox"/> Airline/Airport
B1 <input type="checkbox"/> Banking/Insurance
C1 <input type="checkbox"/> Civil Defence/Emergency Service
C2 <input type="checkbox"/> Coastguard
C3 <input type="checkbox"/> Customs & Excise
C4 <input type="checkbox"/> Security Consultant
C5 <input type="checkbox"/> Communications/Computing
C6 <input type="checkbox"/> Close Protection
D1 <input type="checkbox"/> Defence
D2 <input type="checkbox"/> Diplomatic Corps
D3 <input type="checkbox"/> Distributor/Agent
G1 <input type="checkbox"/> Government
H1 <input type="checkbox"/> Hospital/Laboratory
L1 <input type="checkbox"/> Library
L2 <input type="checkbox"/> Leisure Industry
M1 <input type="checkbox"/> Manufacturing
O2 <input type="checkbox"/> Offshore/Nuclear/Power
P3 <input type="checkbox"/> Police/Law Enforcement
P4 <input type="checkbox"/> Ports/Shipping
P5 <input type="checkbox"/> Prison
R1 <input type="checkbox"/> Research & Development
R2 <input type="checkbox"/> Retail Industry
T1 <input type="checkbox"/> Transport
T2 <input type="checkbox"/> Training
O1 <input type="checkbox"/> Other
PURCHASING AUTHORITY
20 <input type="checkbox"/> Authorise
21 <input type="checkbox"/> Specify
22 <input type="checkbox"/> Advisory
23 <input type="checkbox"/> Other
NUMBER OF PEOPLE IN YOUR ORGANISATION
40 <input type="checkbox"/> 1 – 9
41 <input type="checkbox"/> 10 – 49
42 <input type="checkbox"/> 50 – 99
43 <input type="checkbox"/> More than 100

Please return this completed form to:

Subscriptions, Albany Media Ltd, 74 Albany Villas, Eastworth Road, Chertsey, KT16 8DR, United Kingdom
Tel: +44 (0)1932 566921, Fax: +44 (0)870 4869204, email: subs@intersec.co.uk. Web: www.intersec.co.uk