

Expeditionary Communications for Civilian Personnel

Bjoern Rupp, CEO of GSMK CryptoPhone, sounds a warning of the risks that communication breakdown can entail for civilians who are engaged on overseas operations



The need to encrypt satellite phone communications while working in unstable regions is becoming necessary to ensure safety

Political unrest has spread across North Africa and the Middle East at an alarming rate in recent months. Egypt's revolution has seen millions of protesters taking to the streets in an attempt to overthrow (now former) President Hosni Mubarak, which at times resulted in violent clashes. Tunisia experienced an intense campaign of civil resistance that led to a state of emergency being called, and Bahrain has been rocked by weeks of anti-government protests. But undeniably the most explosive conflict has been in Libya, where Colonel Muammar Gaddafi has waged a war against an anti-government uprising, resulting in the deaths of hundreds of people.

Foreign civilians have been involved in these events for a variety of reasons. The military has intervened, tourists and foreign workers have been stranded, human-rights organisations have been dispatched to help and the media has been reporting from the heart of the action. For all of these people, contact with their home country has been of paramount importance.

Intelligence agencies have invested large sums of money in technology that intercepts calls and records them

A matter of life or death

A United Nations (UN) resolution has called for all states to protect Libyan civilians and a coalition of British, French, US and other forces has been enforcing a 'no-fly zone' over the troubled country. The UN has also intervened in the Ivory Coast, where civil war has broken out after the country's election.

For the scores of foreigners trying to organise themselves in these countries, communication has been a real problem. Governments have deliberately shut down mobile phone networks to prevent their opponents from communicating.

Egypt had a mobile phone blackout for several days, and Libya was also accused of blocking overseas calls temporarily. This has had an enormous impact on people trapped in these countries, leaving them cut off from their contacts at home.

Another key concern is traceability. Intelligence agencies in these countries have invested very large sums of money in technology that intercepts



A Libyan opposition member checks his satellite phone as Misratah looms in the distance

calls and records them. As various regimes try frantically to stay in control, they are even more desperate to trace people's calls and movements. Even the smallest countries have technology capable of monitoring telephone call patterns and raising an alarm when they deviate from the norm. Routine information can be pieced together to paint a picture of who is talking to whom, where they are heading and what they may do next.

Worryingly, the law on phone interception is inconsistent across the world. In many countries it is frequently 'lawful' to intercept calls at will. The technology for interception is available on the open market and is widely deployed, even in the poorest areas of the world. As data storage becomes cheaper, there is almost no limit on how much call information can be recorded.

Protecting yourself

There are dozens of foreign organisations that have a vested interest in being in these countries. But when you have to deploy your workforce to these dangerous regions, safety has to be the number one issue. Whether the objective is for charity, military, media or any other reason, going in underprepared cannot be an option. What happens when the main network goes down?

In these turbulent areas, when aid agencies are moving their people around and there is uncertainty about who is in control, it is possible for anyone to be swept up in trouble. For instance, British and American representatives from Amnesty International and Human Rights Watch were recently targeted – with military police storming their meeting and detaining them for days. How their location was revealed is unclear, but the importance of being able to speak without being traced in these volatile environments is obvious.

The technology for interception is available on the open market and is widely deployed, even in the poorest areas of the world

Ways around the problem

When employees work in unfamiliar territory they are at an increased risk. Traditional mobile devices cannot stop users' phones from being monitored, and the threat of networks going down can leave users vulnerable. But it doesn't have to be this way – tailored and unbreakable encrypted phones exist that use satellite technology to make confidential calls anywhere and at any time. These solutions use strong encryption algorithms and telephones that have been hardened against outside attacks, thus providing 360-degree end-to-end security and preventing calls from being intercepted and locations recorded. They can be linked to a satellite terminal through a wireless LAN connection, and calls can be made independently of unreliable local mobile phone networks.

Clearly, there is a steep learning curve for those in charge of managing security measures, but the threat of phone interception undoubtedly exists and is growing. In the light of this, phone correspondence cannot be overlooked in an organisation's security armour. ■