

Using secure communications in turbulent territory

by Bjoern Rupp, CEO, GSMK CryptoPhone

The Arab Spring brings in its wake serious security issues, for foreign agencies and local activists alike. While Lawful Interception regulations vary in different countries in the regions, there have also been examples of politically motivated shut down of the Internet and mobile communication networks during riots. Providing a secure means of ongoing communication in the face of such turmoil is paramount. The personal security of staff in the region must be protected by unimpeded communication links, such as that delivered by satellite. The information conveyed in such communication must be protected by unbreakable encryption algorithm.



Dr Bjoern Rupp is the Chief Executive Officer of GSMK, the technology leader in mobile voice and message encryption. He has over fifteen years of experience in the telecommunications industry.

Previously, he held a management position at a major global management consulting firm, specializing in strategy development for the Telecommunications, Information Technology, Media and Electronics (TIME) industries.

Dr Rupp studied Economics at the University of Heidelberg, Humboldt University Berlin, and the University of California at Berkeley.

He is the author of several journal articles and book chapters on Internet economics, satellite communications systems, and mobile communications devices.

Communications in Africa and the Middle East have been severely disrupted in recent months as a result of political unrest, which has been spreading rapidly across the region. Egypt's revolution saw millions of protesters taking to the streets in an attempt to overthrow President Mubarak, sometimes resulting in violent clashes. Tunisia experienced an intense campaign of civil resistance that led to a state of emergency being called. Bahrain has been rocked by weeks of anti-government protests, and an explosive conflict is raging on in Libya.

Foreign citizens 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 countries and colleagues is of paramount importance.

A UN resolution has called for all states to protect Libyan civilians and a coalition of British, French and US forces has been enforcing a 'no-fly-zone' over the troubled country. The United Nations has also intervened in the Ivory Coast, where civil war has broken out following 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 in an attempt 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 impacted the workers 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 huge sums of money into technology that intercepts calls and records them. With various regimes frantically trying to stay in control, they are even more desperate to trace people's calls and movements. Even the smallest countries have technology that is 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 a dictatorship 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.

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. Imagine if your staff were cut off from contact because the main network went down? Or they were taken hostage and could not raise the alarm?

In these turbulent areas, when aid agencies are moving their people around and there is uncertainty over 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 high-level 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. On another occasion earlier this year, British photographer Anton Hammeri was shot and killed when he was captured by pro-government forces in a remote area of Libya. Other foreign journalists with him were held for six weeks before being released in May.

When employees are working in unfamiliar territory they are at an increased risk. Traditional devices do not have the capability to protect users from their phones 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.

In the light of recent events, every organisation sending personnel out to these volatile areas should be protecting them from outside threats. While companies are tightening IT security by installing sophisticated software packages, they must also take heed of the vulnerability of voice communications. If traditional interception channels are now closing, adversaries will increasingly target unprotected voice conversations to obtain confidential information and infer an organisation's moves and intentions without detection. Voice correspondence is almost always an uncharted territory for organisations under the false assumption that phone hacking is a highly sophisticated and expensive means of attack.

The days of telephone interception involving expensive equipment and an extensive army

of technology experts are long gone. Only in December it was revealed that a computer engineer had broken the algorithm used to encrypt the majority of the world's digital mobile phone calls online, and published his method, in a bid to expose weaknesses in the security of global wireless systems.

As interception technology gets cheaper and more sophisticated, we can only expect illegal interception to increase. Furthermore, with data storage getting more accessible and cost-effective, an infinite amount of information can be logged, stored and accessed for years to come.

Obviously, there is a steep learning curve for those in charge of managing security measures, but be under no illusion - the threat of phone interception does exist and is growing. In light of this, phone correspondence cannot be overlooked in an organisation's security armour. ●

