Covert Communication Techniques used by Next Gen High Tech Terrorists

Harshal Patel
MS (Digital Forensics & Information Assurance), Institute of Forensic Science, Gujarat Forensic Sciences University

Santosh Khadsare
Head, Cyber Forensic Lab, Delhi

M. S. Dahiya
Director, Institute of Forensic Science, Gujarat Forensic Sciences University, Gujarat

Nilay R. Mistry
Asst. Prof. and PG Course Coordinator, Institute of Forensic Science, Gujarat

"While a terrorist has his fingers on the trigger, his children have their fingers on the mouse."

Abstract : Until now people have fought for food, water or territory, but today the definition and motivation of fighting is changed i.e. terrorism. Terrorists often strike soft targets such as innocent citizens and government infrastructure. The aim of terrorists is to turn people against the government. Terrorists are ahead of the Law Enforcement Agencies to adapt to latest changing technology and use it as a medium to spread terror across the globe. In the recent past, terrorists had been physically present to carry out act of terrorism. But with the advent of technology, they have changed their strategies and converted themselves into high tech & sophisticated groups. They have their own cyber cells and command & control centers which are used to monitor and control their activities. The means of communication with their activists have changed form a courier to use of internet, especially the social media. They attract youths to join the terrorist groups and motivate them for terror activities using wrong interpretation about religion. This article throws light on covert communication techniques used by terrorists to communicate using various techniques.

Prologue

The increased dependency on communication and data networks, storage of information in cyber domain and their vulnerabilities to outside world, lack of mutual consent between countries on effective control of operations in cyber domain has brought a new type of threat. Cyberspace; the fifth space of warfare after land, sea, air, and space is all about the computer networks in the world and everything they connect and control via cable, fiber-optics or wireless. The internet is used for interconnecting people including terrorists who are amongst the first to use the latest technologies even before the government agencies.

The Hyderabad Police arrested three students on 26 Dec. 2015 for allegedly planning to join terrorist group. 'Youtube' was used as a communication medium to seek help. In another case, Delhi Police on 29 Dec. 2015 arrested a former Indian Air Force official from Punjab for allegedly sharing secret documents with other country after he was "honey trapped" by a woman with links to the spy agency. He was allegedly introduced to the spy ring by an unidentified woman whom he had met over a social networking site and shared information through a fake 'Facebook' account.

In May 2015, when two terrorists attempted to kill a whole bunch of people in Garland, Texas, they were stopped by local law enforcement and it was revealed that in the morning one of those terrorists exchanged 109 messages with an overseas terrorist. The government agencies replied, "We have no idea what he said because those messages were encrypted. That's a big problem, and we have to grapple with it." So here encryption played a role in obstruction and helped in secure communication between the terrorists. In Paris Massive attack encrypted communications via TOR and social media were used. For communication purpose they used Telegram like apps, which securely communicate the messages to the other group members involved in that attack.

During Mumbai attacks in November 2008, terrorists used GPS based maps; Satellite based phones for the communication purpose and live telecasts to monitor the event. The communication medium changed during every stage of the attack. Thus it became very difficult for the Law Enforcement Agencies to hunt them down.

Study has shown that the commonly terrorists communicate through normal network channel using secret encoding techniques, which may not be traced out by Intelligence agencies i.e. Steganography and Hidden watermarking. These techniques with high tech encrypted communication may not be traced out through interception. They have analyzed the various social media platforms and categorized them so that their sympathizers can use these platforms with caution.

Practical Case Study Scenarios

High tech terrorist groups are using techniques such as steganography and water marking for communicating covertly with each other. Some of the examples are discussed here with actual implementations.

Add Message to Foreign Language Movie's Sub Titles

Security & intelligence agencies received a report that a suspected person associated with a terrorist group and now probably a sleeper cell was planning a terrorist activity in the coming days. An investigation agency confiscates the digital devices form suspect's house. They recover many files from the suspect's external hard disks. After digital forensic investigation they could not gather any information about the activity planned. They had found some sticky notes with numbers of his home phone and writings such as 00,45,55 scribbled on them which lead the investigation team nowhere. They also found some movies, which were in foreign language, but at the time of forensic investigation they had ignored them. But one of the investigators found one doubtful scene which was the part of that Chinese movie. He played a movie many times with its English subtitles. With available information acquired form investigation the investigator put all things together and trying

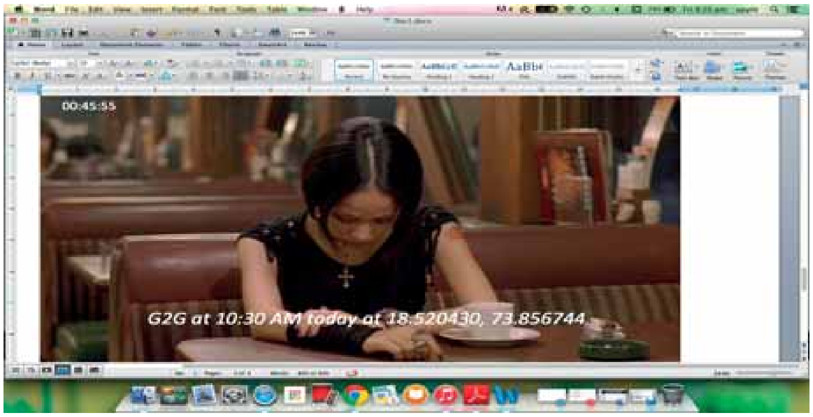

Fig. 1: Still frame from Foreign Movie with Subtitle and Number 004555

to create the intelligence. He analysed all information like movie, numbers and dates, names of folders etc. As a result investigator found below mentioned frame from movie at time 00:45:55.

Investigator found subtitle at 00:45:55 with no voice behind it. Subtitles are normally synchronized with voice and conversations during movies. But this subtitle had no conversation or voice behind it. After getting this evidence they crack down the meaning of message. That message was regarding next Get 2 Gather (G2G) of the sleeper cell group at location mentioned as GPS coordinates to create plan for next target. The GPS coordinate (18.520430, 73.856744) mentioned in sub title of the movie was of German Bakery, Pune, India.

DTMF & Morse Code for Covert Communication of Code Exchange

A person was recently identified as a suspected terrorist. He was suspected of stealing missile activation codes from the Air force, which were handed to officials for a brief period of time. If suspect misuse the code then Air force may have to face some serious trouble. Thumb drive of Tom was found in formatted state and the same was used to store the activation code. Fortunately, system had made a backup image of the drive. One of the Investigators handled this case, for getting activation code details.

The file name was win7.bak, which was back up of windows FAT file system machine. Investigator created an image file of that backup file for fetching potential artifacts.

Thus, investigator successfully fetched the activation code detail from the above-mentioned code.

Barcodes or QR Codes for GPS Coordinates or Location, Map, Auto Message

Barcode generally have 12- to 20-digit number. It is primarily used for serial numbers, pricing and inventory control of the products worldwide. The most common barcode in North America is the 12-digit Universal Product Code (UPC) code. UPC codes used with groceries and books and could be used to track any merchandise if needed. Marketers track consumer choices by analyzing what they are purchasing. With the advent of free barcode scanners on mobile devices, marketers can also pinpoint what age groups are buying what.

But barcode or Quick response code may also be used for communication

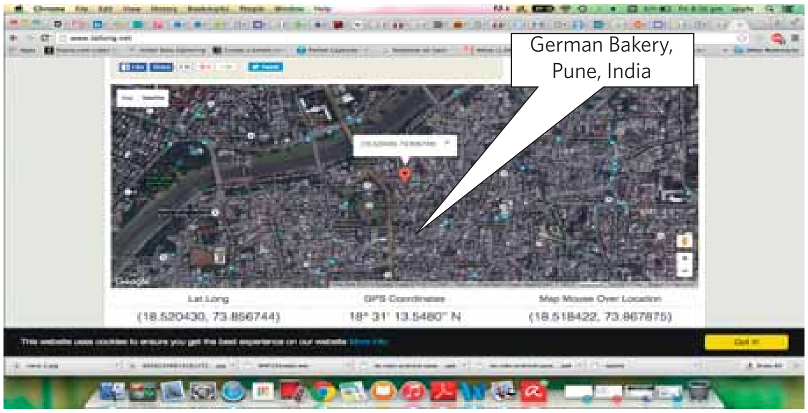

Fig. 2: Location Coordinates 18.520430, 73.856744

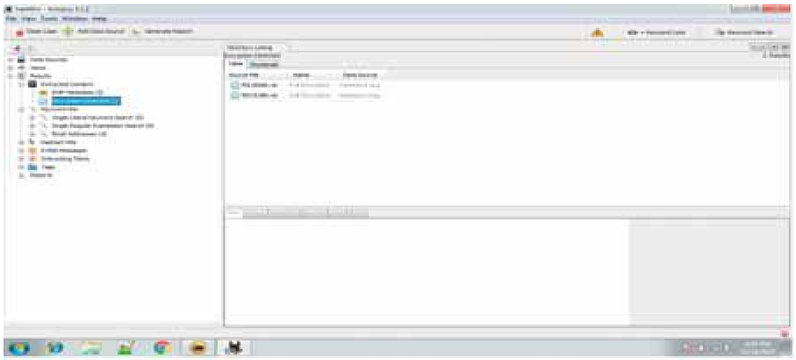

Fig. 3: Found Encrypted Archive File

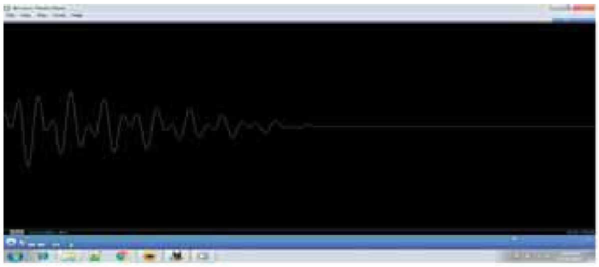

Fig. 4: DTMF Code audio file is there In Encrypted Archive File

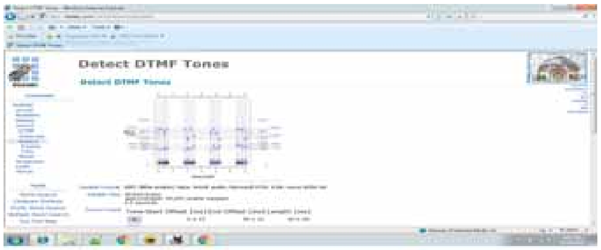

Fig. 5: DTMF Code is Decoded

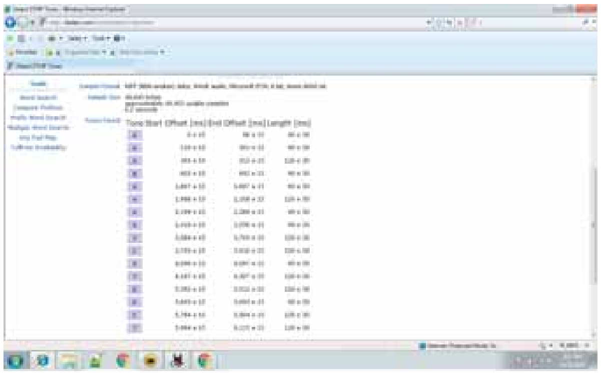

Fig. 6: The Code is Decoded i.e. AA6B A4A8 3C67 DDC7

too. If any terrorist group wants to communicate via covert communication, they can use this technology as a secure message passing system. Figure below shows the meeting will be held at Theatre Royal at 24 February 2016.

Fig. 7: QR Code of meeting place

Conclusion

Thus, from the above case studies, it can be understood that terrorist can use high-tech medium of covert communication channels for passing their secrete messages to their group members. It is also important that investigator should have out of the box thinking capability to understand the modus operandi and technology. Secret is no more secret when it comes to proper intelligence and applying novel detection strategies to identify the secrecy.

Suggestions for Readers

This research paper is presenting covert communication used by criminals. Software sometimes fails to detect the covert communication. In such cases investigator has to apply intelligent approach for decrypt communication.

References

[1] Stevens, T and P R Neumann (2009) "Countering Online Radicalization: A Strategy for Action" (London: ICSR/ Community Security Trust), p. 10.

[2] Corman, S R (2011) "Understanding the Role of Narratives in Extremist Strategic Communications," in: L. Fenstermacher and T Leventhal (Eds.) *Countering Violent Extremism: Scientific Methods and Strategies* (Wright-Patterson AFB, OH: AF Research Laboratory), pp. 36–43;

[3] Cornish, P, J Lindley-French and C Yorke (2011) *Strategic Communication and National Strategy: A Chatham House Report* (London: Royal Institute of International Affairs);

[4] http://globalcenter.org/wp-content/uploads/2013/03/Feb2013_CT_StratComm.pdf.

[5] Casebeer, W D and J A Russell (2005) "Storytelling and Terrorism: Towards a Comprehensive 'Counter-Narrative Strategy'," *Strategic Insights* 4(3),http://www.ciaonet.org.wam.leeds.ac.uk/olj/si/si_4_3/si_4_3_caw01.pdf;

[6] Homeland Security Policy Institute (HSPI) and the University of Virginia Critical Incident Analysis Group (CIAG) (2007) *NETworked Radicalization: A Counter-Strategy*, available from:http://www.gwumc.edu/hspi/policy/NETworkedRadicalization.pdf;

[7] Quiggin, T (2009) "Understanding al-Qaeda's Ideology for Counter-Narrative Work," *Perspectives on Terrorism* 3(2), 18-24;

[8] Qatar International Academy for Security Studies (QIASS) and The Soufan Group (2013) Countering Violent Extremism: The *Counter-Narrative Study*, available from: http://soufangroup.com/countering-violent-extremism-the-counter-narrative-study/.

[9] Presidential Task Force (2009) *Rewriting the Narrative: An Integrated Strategy for Counterradicalization* (Washington, DC: The Washington Institute for Near East Policy);

[10] National Coordinator for Counterterrorism (Ed.) (2010) *Countering Violent Extremist Narratives* (The Hague: National Coordinator for Counterterrorism); Home Office (2011) *Prevent Strategy* (London: The Cabinet Office).

[11] Archetti, C (2012) *Understanding Terrorism in the Age of Global Media: A Communication Approach* (Basingstoke: Palgrave).

[12] http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/11038121/David-Cameron-Isil-poses-a-direct-and-deadly-threat-to-Britain.html); (Blears, H and J Lewis (2014) "Jihadists Need to Be Treated Like Nazis," *The Times*, 27 August).

[13] Stevens, T and P R Neumann (2009) "Countering Online