Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
13/16

EXPLOITATION OF SOCIAL MEDIA BY ENEMY: HONEYTRAP OPERATIONS

Ms Kriti Singh
Assistant Professor
School of Media Studies
Jaipur National University

"When one with honeyed words but evil mind
Persuades the mob, great woes befall the state."
- Euripides, Orestes

On 17 Jan 2016, in the backdrop of recent Pathankot attack by terrorists, Defence Minister Manohar Parrikar assured that, "The government is taking all measures to prevent military personnel falling prey to foreign intelligence agencies." The statement again highlights the threat coming from one of the most amorous arts of deception and enticement, known as honey trap operations. Recent media reports reveal that the enemy sitting across the border is unceasingly masterminding honey trap operations and this time using the social media platforms.

The history of 'honey traps' also known as 'honey pots' is as old as the history of espionage and is considered as most successful espionage tactics. Perhaps the earliest honey trap on record was the betrayal of Samson by Delilah, who revealed Samson's weakness (his hair) to the Philistines in exchange for 1,100 pieces of silver, as described in the Book of Judges. The practice continued into the 20th century and became a staple of Cold War spy craft.[1]

The term 'honey trap' refers to use of a strategy, which involves appealing and beautiful people, equipped to deceive the target and acquire the desired objective, which can be getting a vital piece of information or an action. According to the encyclopedia of Cold War Espionage, Spies, and Secret Operations, "A honeytrap is an operation aiming to recruit agents to the secret service with threats to expose their romantic or illicit sensual intimacies and thereby wreck reputations; it is also a means of getting intelligence on foreign nations by using seducers instructed to inform their customers."[2]

The recent example of the defence personnel enticed into the honey trap, to extract information provides us a few lessons to learn. Firstly, in order

to entice the target, social media Facebook was extensively used. This episode again exposes the vulnerability of these social media platforms and how the enemy can disguise himself into an 'innocent looking media person seeking information for a magazine article.' Secondly, it again presents before us the peril of establishing contact with 'unverified source' and talking to 'media person' without proper permission, thus resulting into the leakage of information. Thirdly, it reiterated the fact that any small information, pertaining to the unit, troop movements, location, equipment, etc., is not something to boast about, or share on social media platforms. Forgetting the basic principle of maintaining 'silence' with regards to official communication and information can result in a security dilemma for a nation.

Fourthly, the incident also saw the usage of communication apparatus like Voice Over Internet Protocol-based calls, e-mails, Internet-based text messaging services, etc. by the enemy. The advancement in technologies has brought sophisticated equipment with simple operations in our hands. But if not used wisely, it can prove counter-productive. Investigations so far have revealed how Skype, WhatsApp etc., were extensively used in exchange of information, in lieu of money and pleasure. Lastly, one can also see how divulging one small seemingly irrelevant piece of information, to an unknown person, one meet's 'online', can let one into a vicious circle, where extracting of simple information can gradually turn into extraction of crucial information.

There is no denying that communication technologies have changed our lives. Nevertheless, like every coin has two sides, these technologies also come with dual uses. It is a bitter truth that the emergence of the social media networking platforms, which has compressed the time and distance barrier, is proving itself as a breeding ground for honey trap operations. The penetration of this invisible web of honey traps is yet to be assessed. According to Indian security agencies, "Inter-Services Intelligence (ISI) has been using social networking sites such as Facebook and Twitter to honey trap unsuspecting Indian personnel by providing training to women on how to make explicit calls and chats, in a field traditionally dominated by men. The lure begins with friend requests."[3]

While elaborating on the modus operandi adopted by the adversary, to trap defence personnel, a senior officer investigating the ISI spy network revealed, "The moment an officer discloses his online identity, he/she comes on the radar of spies who starts following him on the virtual world....They (spies) also keep a track of their interest and hobbies to make a conversation and get friendly. Spies have created many a fake profile and identity on social media and use it according to their targets."[4]

Another trend, which has been exposed lately, is the abuse of social media by enemy to trap veterans' in the garb of providing job opportunities and financial aid. The Home Ministry has conveyed that a fake organisation of ex-servicemen was

formed in North India, which promised job opportunities and financial assistance to the former soldiers. The promoters of the organisations even asked some former soldiers to get in touch with their serving colleagues and try to gather information about field formation, raising suspicion among the ex-servicemen.[5]

These incidents have exhibited how the adversary is manipulating and capitalising on the lethal side of social media. The bigger challenge lies in the fact that more than thousands of personnel working for defence and security establishments are somewhere directly and indirectly connected to social media. While revealing the level of training given to the honey trappers by ISI, a senior official with the central security agency, "Our investigation has revealed that ISI has set up a cyber wing equipped with modern technologies for massive online tracking. They are giving voice training to agents to appear more professional while dealing with defence personnel online."[6]

To conclude, Dutch Renaissance humanist and theologian, Desiderius Erasmus, once said, "Man's mind is so formed that it is far more susceptible to falsehood than to truth." These words of early 16th century theologian still hold ground in the 21st century. Despite being aware of the truth that how social media platforms can be exploited, still we fall in the web of enticement. The recent examples reveal the lethal side of social media. The answer lies in remaining vigilant and selective about the information one share on social media platforms and as Defence Minister Manohar Parrikar noted, "Honey traps could be avoided by being alert."[7]One has to understand and practice the demarcation between personal and professional life and bear in mind already framed guidelines and code of conduct, while accessing social media platforms. It's better to be safe than sorry.

Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1]"Honey Traps: Intelligence Business Is the Oldest Profession…." *Passivevoices*. Accessed January 26, 2016. https://passivevoices.wordpress.com/2012/09/12/honey-traps-intelligence-business-is-the-oldest-profession/.

[2]Trahair, Richard C. S., and Robert L. Miller.*Encyclopedia of Cold War Espionage, Spies, and Secret Operations*. New York: Enigma Books, 2013.

[3]Shashank, Shekhar. "ISI Laying Honeytraps on Facebook and Twitter to Snare Indian Defence Personnel." *India Todau*, January 3, 2016. Accessed January 26, 2016. http://indiatoday.intoday.in/story/isi-laying-honeytraps-on-facebook-and-twitter-to-snare-indian-defence-personnel/1/561137.html.

[4] Ibid

[5]"MHA Alerts MoD on 'spy Ring'." *Dailyexcelsior*, December 31, 2015. Accessed January 26, 2016. http://www.dailyexcelsior.com/mha-alerts-mod-on-spy-ring/.

[6] Ibid.n3

[7]Dinakar, Peri. "Steps Being Taken to Prevent Honey-traps, Says Parrikar." *The Hindu*, January 17, 2016. Accessed January 26, 2016. http://www.thehindu.com/news/national/steps-being-taken-to-prevent-honey-trap-cases-parrikar/article8113591.ece.