"Traditional collection tools and techniques used by the intelligence community are obsolete" – A critical analysis

A number of terrorist attacks, such as the 9/11 attack on the Twin Towers, have pushed all nations to gear up and devise tools and tricks for collecting sensitive information with regards to the security of the nation. However, it seems that our current age-old methods might have a number of loopholes which enables terrorists to fool the Intelligence Agencies and wreak havoc in a country. This paper aims to review some of the traditional techniques for gathering intelligence and some of the possible disadvantages associated with each of them.

In order to understand the intelligence measures taken by the security forces, it is imperative to first understand the changing trend of terrorist attacks and their means of deceiving the security forces. In our current digital age, it is quite easy for terrorists to gather information, change their identities, and collaborate with their fellow members in planning an attack. According to the Security for Business Innovations Council, the advanced threats facing the world today are cyber-attacks, where the main objective is stealing intellectual property, planting false information and monitoring internal operations. At least 855 instances of security breaches have been reported in 2011, according to the Verizon 2012 Data Breach Investigations Report (Weber, 2012).

Terrorist attacks, such as the one that took place in September, 2001, is another major concern for intelligence agencies and a matter that needs to be looked into immediately. Such attacks present more of a threat as it is a matter of life and death for thousands of people. Hence, it is extremely critical that law enforcement agencies use intelligence for the prevention of crimes, both locally and nationally. The biggest indicator for any intelligence measure to be effective is how widely it is able to cover an organization's activities. However, it is not practical

for many organizations to spend a large amount of resources on intelligence gathering. Hence, based on the time and money it can spend on intelligence gathering, each organization needs to customize strategies for its own security (Peterson, 2005). Given below is a discourse on strategies used for intelligence gathering currently, including its advantages and disadvantages.

One important strategy that was developed in Britain to counter crimes like automobile thefts and burglaries is intelligence-led policing. In this, members of the police force monitor calls to gather information and then use this information to obtain leads of criminals and/or terrorists. This technique has also worked well in the United States where information is passed on to detectives, patrol officers, management and other anti-terrorist organizations for further analysis. Another strategy that also originated in the United Kingdom is the National Intelligence Model. In this model, a particular crime, such as terrorism, is prioritized and then targeted strategies are developed based on the current level of threat and resources available for gathering intelligence. A similar strategy developed by Herman Goldstein is problem-oriented policing. Here, the problem at hand is analyzed in detail and then a suitable strategy is developed to tackle that particular issue. It requires the testing of a number of different solutions based on the location and the political environment of a region (Peterson, 2005).

All the above mentioned strategies use one or more of the conventional intelligence gathering techniques. The most basic one of these is patient and painstaking observation and analysis of open sources, coming to conclusions and transferring the information to the relevant organizations. This information is then analyzed by the organization members and further action is collectively decided. However, this method yields a large number of false positive results which ultimately leads to a waste of valuable resources (Nte et al., 2010).

Hence, in order to overcome the disadvantages of the above intelligence gathering technique and to improve the credibility of the information collected, a scientific and mathematical method was devised to gather sensitive evidence. However, there is still uncertainty associated with this method and more tests need to be run on this information to test its validity. These include probability distributions and calculation of their means, application of parameter estimation theory to assess the quality of the information collected, calculation of information entropy and calculation of Bayesian estimate. In spite of all these measures used for the validation of the intelligence obtained, this method runs a high risk of failure as it is quite open to errors and manipulations (Nte et al., 2010).

With the advent of the technological age and the perceived disadvantages of the conventional intelligence gathering techniques, a number of technological methods have also been developed for gathering intelligence. Human Intelligence (HUMINT) is collected when officers are sent as spies to foreign countries to gather valuable information. As this is purely human effort, it requires a lot of time and effort and is not as reliable as advanced scientific technology. It is also very difficult to teach and to learn and officers going to foreign countries need to take tremendous efforts to learn their language and culture. These spies are also more vulnerable and susceptible to deceptive practices (Margolis, 2013).

Another type of intelligence gathering technique is Signals Intelligence (SIGINT) which involves gathering information by the analysis of foreign electronic communications. A similar type of strategy, Communications Intelligence (COMINT) also involves gathering intelligence from various means of communication. However, both these strategies require that communication between attackers occur such that it can be intercepted and analyzed for valuable

information. Also, decrypting a coded message is quite a difficulty for communication analysts (Margolis, 2013).

More advanced techniques for gathering intelligence are Electronic Intelligence (ELINT) and Telemetry Intelligence (TELINT). ELINT involves obtaining information from electronic emissions and TELINT involves obtaining information from signals given off weapons. Although these ward off the vulnerabilities involved in HUMINT, there are still a number of disadvantages associated with them. In most cases, terrorists do not release enough signals that can be intercepted and there is always the risk that these endeavors are discovered and they become more wary in the future (Margolis, 2013).

As attackers are becoming smarter with the introduction of advanced technology, it is imperative that a nation's security is also strengthened by leaps and bounds. Loopholes have been identified in most conventional methods of intelligence gathering and have been used mercilessly to deceive nations and launch massive terrorist attacks. The world is currently in dire need of new advanced and intelligent strategies to take care of the security of nations.

References

Margolis, G. (2013). The lack of HUMINT: a recurring intelligence problem. *Global Security Studies, 4*(2), 43-60.

Nte, N. D., Eke, P., & Anele, K. (2010). Rural intelligence gathering and the challenges of counter insurgency: views from the Niger Delta. *Bangladesh e-Journal of Sociology, 7*(1), 21-32.

Peterson, M. (2005). Intelligence-led policing: the new intelligence architecture. *U.S. Department of Justice*, NCJ 210681.

Weber, D. (2012). Transforming traditional security strategies into an early warning system for advanced threats. *RSA Security Brief*, EMC².