Counterintelligence

Name

Institution

Counterintelligence

Counterintelligence could best be described as the technique of gathering data and performing activities aimed at identifying, exploiting, disrupting, or protecting against spying and other related intelligence activities (Redmond, 2010). Such other similar information actions are assassination or sabotage done for or on behalf of foreign countries, firms, people or their agents, or even global terrorist activities or groups. Counterintelligence is also viewed as counterespionage and also a method to validate assets (Kramer & Heuer, 2007). Among the emerging or developing issues and challenges in counterintelligence is the advancement of modern technology. The new technology is increasingly affecting the U.S. counterintelligence operations and activities, hence ought to be addressed.

The impact of modern technology on U.S. counterintelligence is detrimental to the security of the critical government and organizational information. Modern microelectronics and information technology gadgets have been noted to revolutionize almost all other aspects of human existence; hence, there is a high chance of the same having considerable impacts on counterintelligence. Since the currency or basis of espionage is information, potential leakage of useful data is harmful (Kramer & Heuer, 2007). The new technology has helped in miniaturization of information, thus, potentially reducing the risk of detection and ultimately increasing the overall productivity of any agent. However, theft of such a gadget carrying the essential information has profound implications for national security.

With the revolutionary change in the diffusion of information, a slight mistake such as spelling error could sabotage the safety of the nation. However, this depends on the computer safety standards in place. For instance, an agent can retype classified information and send it to an unclassified electronic mail system, hence, exposing it to the entire world within a short period. The internet is the primary product of modern technology, and it presents substantial impacts to the U.S. counterintelligence. The web's vast information, and which is cached from previous years or that which is directly accessible offers opportunities to foreign intelligence agencies or determined individuals, hence, they can quickly discover U.S. classified information. As explained by Moravej and Diaz (2007), a particular newspaper while searching for a commercial online data service was in a position of creating a directory for over 2,600 employees of the Central Intelligence Agency (CIA). The newspaper further disseminated 50 internal agency phone numbers as well as the physical locations of various secret CIA facilities in the U.S. (p. 61).

Since the internet's major role is rapidly distributing free information, the intelligence firms and security organization are faced with the dilemma of restricting and complicating the access of their information. Any effort by the U.S. government to regulate freely available databases for personal information through implementation of strict privacy laws would have dire implications for the work of the intelligence, since there would be the elimination of the available essential data for their operations (Moravej & Diaz, 2007). In this instance, the advancement of modern technology has been adverse to the mission of the US counterintelligence.

Even though the U.S. is well equipped with devices essential for electronic surveillance, other foreign intelligence services and private organizations are also increasingly investing on the same. However, most employees, particular the elder generations of the organizations involved in security and counterintelligence do not have the adequate technological knowledge, or they do not have the ability to ensure that information is highly secured (Moravej & Diaz, 2007). As elaborated by Moravej and Diaz (2007), foreign counterintelligence agencies, i.e. that of China have highly skilled employees who are experts of attacking and breaching the electronic security, even of the most conscious organizations like that of the United States. As explained by Moravej and Diaz (2007), on numerous occasions there have been electronic attacks from China (with the code name Titan Rain) which have managed to breach the networks of the U.S. agencies and the Department of Defence (p. 62).

However, apart from adverse impacts of technology on the mission of the US counterintelligence, there are various benefits associated with the same technology. With the increased development and dissemination of communication and information technologies, embattled states have ensured that there are multiple platforms necessary to facilitate the flow of information from the public (Shaver, 2016). However, the tipping platforms are at times subject to terrorist sabotage; hence, the information is not secured. Nonetheless, the established tipping platforms ensure that the residents of affected areas, particularly in the time of terrorist attacks, find a channel to report terrorist organization (Shaver, 2016).

Similarly, the Pentagon has proposed a techno-surveillance system known as the Total Information Awareness (TIA). The TIA will use supercomputers as well as sophisticated software and data-mining strategies that are common in marketing and, thus, maintain records on credit card purchases, e-mails, prescriptions, plane flights, rental permits, and such related activities all aimed at detecting suspicious activities (Gerdes, 2004). The TIA will be significant in the prevention of such questionable actions like a purchase of certain dangerous chemicals and also the rent of planes that could be intended to dust crops.

However, the US counterintelligence ought to consider the legal requirements in its operations aimed at detecting malicious activities. There is the need to acknowledge that each citizen is entitled to privacy; hence, the invasion of the same is not allowed. In efforts of collecting, integrating, and evaluating large amounts of personal data on all U.S. citizens, the government will have infringed and compromised the privacy and political liberty of its citizens (Gerdes, 2004).

Ethical Issues Regarding Technological Advancement and U.S Counterintelligence

The handling and processing of the different categories of personal and private information by the U.S. counterintelligence are faced with various ethical issues. The agencies must address the issue of compromising the personal and political liberty of the U.S. and other states' citizens in its operations to counter espionage and other related activities such as terrorism. First, the agents should decide which categories of private and personal data is supposed to be gathered. This question is of utmost essence to infopreneurs. The other ethical issue is the confidential treatment of the information gathered. The U.S. counterintelligence agency should ensure that the personal details tapped should not be used for other purposes other than the primary objective for which it was specifically gathered (Gerdes, 2004). The issue discussed is also related to the rights of an individual regarding the use and distribution of personal and private information. The process of bugging personal electronic gadgets such as smartphones and personal computers. The issue of freedom is most often compromised when the counterintelligence team secretly acquires personal information. A person is entitled to the freedom to make the choice regarding freedom of privacy as well as being free from intrusion. However, the U.S. counterintelligence is protected by the legislation that an individual's choice of privacy should not restrict the freedom of others.

References

Gerdes, L. I. (2004). *Espionage and intelligence gathering.* Farmington: Greenhaven Press.

Kramer, L. A., & Heuer, R. J. (2007). America's Increased vulnerability to insider espionage. *International Journal of Intelligence and CounterIntelligence, 20* (1): 50-64.

Moravej, K., & Diaz, G. (2007). Critical issues in contemporary counterintelligence. *UNISCI Discussion Paper , 13* (1): 53-70.

Redmond, P. J. (2010). The challenges of counterintelligence. In L. K. Johnson, *The Oxford Handbook of National Security Intelligence (pp. 537-54).* New York: Oxford University Press.

Shaver, A. (2016). Information and communication technologies, wartime informing, and insurgent violence. *Counterintelligence*, 1-43.