The role of federal agencies in fighting digital crime

Law

The Role of Federal Agencies in Fighting Digital Crime This paper discusses a number of law enforcement departments in the United States that have taken up the roles to fight computer crimes and terrorism. Additionally, it analyzes the challenges that have existed pertaining to the nature of these agencies and the factors that are common to each of them. The paper further gives suggestions on how to curb these crimes.

Introduction

In the current digital world, online communication has become the norm, users of internet and government institutions have accelerated the possibility of being targeted from the cyber crimes normally associated with the computer world (Stohi & Grabosky, 2010).

With the increase of cyber crimes and cyber criminals, the development and advancement of techniques has influenced the shifting of computer crimes and terrorism from thievery of financial information to surveillance on businesses and pushing into the access of government information (Malkin, 2002). There has been dire need for any states especially the United States to come up with ways of curbing these kinds of crimes in the recent past as it threatens national security and creates opportunity for distortion of technology. To fight this kind of crime that is slowly digging into the modern technology, there must be the presence of heavy security and anti –crime agencies. They include Secret Service, FBI, and Department of Homeland Security among other agencies (White, 2012).

However, these law enforcement agencies have faced a number of challenges in their line of duty. First, the law enforcement agencies themselves are not free of theft or any crime that is associated with

computer because they have also embraced technology and have hence started using and storing intelligence information in the computers (Malkin, 2002). This means that the criminals who perform these kinds of crimes are in positions of destroying what the law enforcement agencies could use to curb them.

Second, the law enforcement agencies have a conflict in the incident and call data, as opposed to community policing. Initially, departments obligated with the maintenance of databases that shows cases that have been reported and call for service provide limited details that do not reflect the quality-of-life issues that affect a particular geographical area. This further translates to communities that are more vulnerable to major crimes because the essence of security involves ground work as opposed to remotely accessing data from the net (Malkin, 2002).

Third, law enforcement agencies have issues with crime mapping, which is the analysis of geographical areas bringing forth problem locations. In particular these agencies lack the skills that are required in data mining and statistics. In essence, Stohi and Grabosky (2010) argue that geographical areas that are vast populated with a high–crime prevalence might turn out to be moderately orderly while the less populated areas may seem to have more of crime scene hence making the mapping to be less reliable.

Fourth, the law enforcement agencies lack total global collaboration in updating domestic laws, legal assistance investigative techniques, and extradition to be at the same pace with the cyber-criminal (White, 2012). In addition, some of the nations lack technical expertise or legislation that permits these agencies to search for evidence in electronic venues before it

has been tempered with or better still to the court when offenders are been tried (Stohi & Grabosky, 2010).

Moreover, the law enforcement agencies have received quite a percentage of rejection from some of the business emperor due to technical power that they are said to have. According to White, 2012, most entrepreneurs' means that once the agencies have gotten valuable information then the government can also get the information and so do other entitles apart from the government leading to business exploitation.

Conclusion

With the expansion, of the internet so has its misuse. Criminals of computers crime and terrorism have the same diversity as compared to the crimes themselves. The war against these crimes must be fought relentlessly since the world can not do without the internet and computers. The United States should come up with strict rules to protect the computer world, as well as introduce stern penalties for those found having committed such kind of crimes.

References

Malkin, M. (2002). Invasion: How America still welcomes terrorists, criminals, and other foreign menaces to our shores. Washington, D. C: Regnery Pub.

Stohi, M., & Grabosky, P. (2010). Crime and terrorism: Los Angeles. Sage.

White, J. (2012). Terrorism and homeland security. Belmont, C. A: Wadsworth Cengage Learning.