The Future of Digital Crimes and Digital Terrorism

[Name of the Writer]

[Name of the Institution]

The Future of Digital Crimes and Digital Terrorism

**Introduction**

 In this modern age, technology has advanced to the peak of development on social, economic or individual levels. This has created a current dispensation impacting every user of information technology. Digital terrorism or crime is a problem which is granted to this world by the progression of internet and information technology. The groups of digital terrorists have turned towards the cybercrime activities related to the infrastructure of U.S security. They have attacked and molested the security system through different ways of hacking by using various tools connected to an internet firewall. Due to the prevalence of cyber or digital crime and terrorism, the law authorities and institutions have recognized the acquirement of security measures needed by the users of the internet. New and innovative ways to burglary are being invented and advanced with the coming time by cyber or digital criminals. Therefore this paper seeks to analyze the means through which law enforcement agencies will combat digital or cyber terrorism and crime.

**Discussion**

**Information Technology Combating Digital Terrorism**

 Information technology has always played an essential role in the economic growth and development of a country. However, it has always been an early adopter for law enforcement agencies to combat digital crime and terrorism. It is considered as a valuable asset for information technology to provide the state or economic system a redefined manner of communication and conduct within the organization. Such that it has opened up new and enhanced ways of dealing and communicating the business, making information technology to impact the global changes throughout the world. However, regardless of the success and development of information technology, it has increased the adverse effects or disadvantages due to the technological invasion. Just because of information technology, criminals have acquired ways through which they lodge attacks through cybercrime and terrorism on the states and authorities.

 The progression of information technology in the 21st century has various advanced parts of society, i.e., communication, computer systems, weapons, brain wave sensors, density scanners, and vision enhancers. It made it a lot easier for managing the atrocities which occurred due to digital crimes and terrorism (Geetha & Phamila, 2016). The information technology along with the computers assists in investigating and analyzing the crimes. For instance, computer forensic determines different techniques in computing like identification, preservation, extraction, interpretation, and documentation, for providing evidence in the court.

**Existing Challenges**

  In the United States of America, the law enforcement agencies on local and federal level include Department of Homeland Security, FBI, and many others which have taken a toll on fighting against the digital crimes and terrorism. The responses and roles of such agencies for law enforcement concern the digital crimes that create challenges limiting the enforcement of laws and regulations against digital terrorism. The evolving challenges which are faced by the Department Of Justice are for instance online child pornography, corporate fraud, mortgage fraud, digital terrorism, and digital crime. Such challenges along with many others have created a rift in combating the crimes and terrorism within the US (Finklea & Theohary, 2015).

 The foremost challenge faced by these agencies is about privacy rights and confidentiality, as people have this perception that if the law enforcing departments scrutinize their online data, then their privacy is at risk. Other challenges might include a lack of training, expertise, resources, and funding to solve a digital crime. Even after many debates of how it will protect the fundamental interests of the common man, it has not won over this argument. As the crime rate has increased so does the innovations and technological advancement, which worsened the things for law enforcing agencies regarding catching the criminal. The criminals have also advanced with this progression, and they use modern technology like e-mail, tweet or any other means of communication to get connected with the world of crime with anonymity.

**Efforts of Federal Agencies**

The challenges mentioned above are the growing concerns of state and local authorities on the dangers made identifying with the security at the federal level about computer infrastructure (Alcaraz & Zeadally, 2015). The officers at locality do not have the understanding or comprehension of digital crimes significant in legitimately searching for the offenses, for example, digital terrorism and crime, theft, violations and misrepresentation, and burglary through digital advancement. Having instruction and proper preparing is critical in the examination procedure to pick up a high ground in battling computerized crimes and terrorism. Consequently, the local and state and law authorities communicated worries about asset requirements and dread concerning aptitude and jurisdiction.

The White House has recently proclaimed the formation of a latest federal agency, known as the Cyber Threat Intelligence Integration Center (CITIC). This is created to direct the intelligence on terrorized threats on the cybersecurity of the nation and devise strategies for combating them. Other federal agencies like the Department of Homeland Security, Department of Justice and National Security Agency are currently working on the prevention and defense against digital crime and terrorism. These agencies are providing the awareness in cyber-situational aspect, and they handle the circumstances related to the practical response, critical infrastructure and mitigation support.

**Key Future Trends**

 The future of digital or cybercrime is way beyond the hacking and damaging the computer data and risking the security. The future is under fire, and safety is at higher risk. However, in spite of the advantages gained by technology it also offers extreme danger and threats. The traditional crime is taken over by cyber crimes in many ways. Now a common theft is not done casually; in fact, the online accounts may get hacked. New and innovative ways to burglary are being invented and advanced with the coming time by cyber or digital criminals. Wherever the law enforcing agencies get to one end of catching cyber criminals, they begin a new one.

 The future trends show that it will not be something only happening on computers or PCs, but it has access to smart devices, small chips, and cards. Cyber hi-jacking, human malware, cyber assault, cyber extortion, car exploiting, brick attacks, identity theft-squared, and mini-power outages are all the newest trends which will take place in the future, more innovative digital terrorism and crime era (Khakzad et al., 2018). Just because of increased dependency on technology, the vulnerability to the cybercrime is inevitable in the future. Future criminals will not face limitations such as skills, physical proximity and daring.

**Conclusions**

 Consequently, this paper analyzed the role of law enforcement agencies in combating digital or cyber terrorism and crime. It has explored the information technology has always played an essential role in the economic growth and development of a country. The progression of information technology in the 21st century has various advanced parts of society, i.e., communication, computer systems, weapons, brain wave sensors, density scanners, and vision enhancers. The future of digital or cybercrime is way beyond the hacking and damaging the computer data and risking the security. Therefore, the local and state and law authorities communicated uncertainties about asset requirements and dread concerning aptitude and jurisdiction. Federal agencies are working on the prevention and defense against digital crime and terrorism. The future trends show that it will not be something only happening on computers or PCs, but it has access to smart devices, small chips, and cards.

**References**

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, *8*, 53-66.

Finklea, K. M., & Theohary, C. A. (2015, January). Cybercrime: Conceptual issues for congress and US law enforcement. Congressional Research Service, Library of Congress.

Geetha, S., & Phamila, A. V. (Eds.). (2016). *Combating security breaches and criminal activity in the digital sphere*. IGI Global.

Khakzad, N., Martinez, I. S., Kwon, H. M., Stewart, C., Perera, R., & Reniers, G. (2018). Security risk assessment and management in chemical plants: Challenges and new trends. *Process Safety Progress*, *37*(2), 211-220.