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**

The violent acts and the use of internet resources that lead to harm or threat for anybody are referred as cyber terrorism. There are various reasons as for why people use online sources and links to attack others. One of the primary purposes is the massive use of technology and the placement of everything on the internet. The second major factor is political, social, economic and ideological. Same is the case with terrorism that is faced by agencies like the Federal Bureau of Intelligence (FBI), Department of Homeland Security and other law enforcement agencies. These organizations are trying their best to combat the threats that are placed by non-state actors and groups across the world. While using the latest technology and the tools of artificial intelligence, they are effectively countering the issues.

**Discussion**

 Various types of hackers use and seize the control of technology for making people vulnerable. The discoveries in the biotech can reach dangers that come from worse than stolen data or the disruption of infrastructure. Printers like 3D help the agencies in finding criminals through the fingerprints which are used in a particular gun. However, there is a potential threat from digital resources as mentioned by the media and international crime agencies (Goldsmith & Brewer, 2015). Various experiences and incidents supported the fact that terrorist groups used the internet for their communication and the recruitment of new members. In April 2007 Estonia a Baltic state continually evolved in terms of advancing technology and became a battleground for the cyber terror of removing the WWII statue which was located in the capital. In response to such type of attacks, there was a concept of counterterrorism generated in the international news media to tackled terrorism.

 Various definitions are underlined by the organization regarding their preferences and need of the time. Central Intelligence Agency of the United States has provided a work plan for creating a separate unit with the name of the counterterrorism department (Harrop & Matteson, 2015). It is motivated by the political cause and the degree of threat underlying public in the United States. With more and more reliance on the internet and online resources, it became evident for the students of digital crimes to understand how the organizations and agencies across the world are considering cyber terrorism as a real threat of the post-modern era. The anonymous groups and the denial of service attack is something very much technical and use for censoring the groups which can attack any professional installations.

 United States Strategic Command and the US Department of defense accomplishing the task of countering these threats through the joint taskforce global network and often use the services of a satellite. The USSTRATCOM well supports the component of operations, and it also was done by the integration of GNO capacity. The actions of all the services and agencies, DoD combat command, systems, networks, and computers are protected well before the attack made by opponents. There was the announcement of creating a separate MAJCOM for Air Force defense and to monitor the internet of America in the cyberspace. Specific laws were also passed by the state to ensure that that person or the entities which are found a suspect in using cyberspace acts would be punished accordingly (Harrop & Matteson, 2015). In 2011 there was a man who was indicted with attacks on US central command with 92 cyber hits, and he hacked the systems that was used by the government organizations.

 The Nebraska-based consortium had apprehended the 4 million hacking attempts in eight weeks which was one of the significant occurrence using internet resources. More than 30 percent of assaults are increasing during the last two-three years. States that are linked with NATO are technically attached with the central networking group to respond to any threat from the non-state and ethnic based groups which are creating trouble for the online users of the internet. The communication of defense authorities and agencies is also not saved unless a proper monitoring system is channelized by the concerned department (Harrop & Matteson, 2015). The conventional network access control is the tool that is used by a government to respond to any threat made by online resources. Defensive tools generally weak because of the attackers approach for moving ahead and creating sophistication for the concerned agencies.

 The nature of war is complicated and challenging, and it shows that a defender is always behind the attackers. One cannot attack the organization or any sources of online concerned without having more knowledge than the target. However the co-practices and coordination among international agencies where they are consistently increasingly skilled level and combating their desired destination. Other than the practical steps, Congress will pass more laws for making and saving the online users of the United States. The state imposed data breach notification requirements where the specific attorney will take necessary action against those who are involved in the breaching of sensitive information. US House of Representatives has drafted a law that will ensure the elimination and much of the responsibilities to be put on the crime related agencies for their effectiveness and making the things simple.

 Among the major initiatives and considerations of state, there must be the reading and investigation of technical concepts that are associated with attacks on digital resources. The description of attacks and the nature of crimes should be disclosed through training and workshops (Mkrtumova et al., 2016). The overview of tactics and legal activities concerning the type of crime and in-depth coverage of investigation can support the war against digital world crimes. The research tools on terrorism should be enhanced to save the data of critical areas and other things. Communication of the various organizations and data that is protected at different places must be supported by the comprehensive software which could deter any threat-related to it. Wilson Center and the US counterterrorism plan ensures effective dealing with international terrorist organizations and ethnic groups.

 According to the reliable sources of United Nation Security Council the future of the digital world might be saved or not but the counter-terrorism strategies are not only useful but resulted in making the American safe. Through various resolutions and acts it is making the digital attacks not to work anymore (Surette, 2015). However, there is a contradiction for states who are not complying the laws and regulating measures issued by the international security agency. Other than United States people across the world have the privilege to find their ways and put most of their burden on the attackers. Committees at various levels are also working to reduce the threat at a maximum position to ensure that the organizations are protected.

**Conclusion**

Concluding the discussion independent nature of law enforcement agencies along with the efforts were taken by US counter-terrorism department are laudable. Fighting computer crimes is not as easy as everything became sophisticated. By following the rules and laws passed by UNSC against the crimes that are prevalent in the digital world, the countries can adequately protect their data. It was the primary concern as emphasized by the Security Council that states are not following the resolutions and laws passed by it.

**References**

Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112-130.

Harrop, W., & Matteson, A. (2015). Cyber resilience: A review of critical national infrastructure and cyber-security protection measures applied in the UK and USA. In *Current and Emerging Trends in Cyber Operations* (pp. 149-166). Palgrave Macmillan, London.

Mkrtumova, I., Dosanova, A., Karabulatova, I., & Nifontov, V. (2016). THE USE OF COMMUNICATION TECHNOLOGIES TO OPPOSE POLITICAL-RELIGIOUS TERRORISM AS AN ETHNOSOCIAL DEVIATION IN THE CONTEMPORARY INFORMATION-DIGITAL SOCIETY. *Central Asia & the Caucasus (14046091)*, *17*(2).

Surette, R. (2015). Performance crime and justice. *Current Issues in Criminal Justice*, *27*(2), 195-216.