Cyber terrorism and warfare

Law

Cyber Terrorism and Warfare Cyber Terrorism and Warfare Cyber terrorism and warfare involve use of a computer network to tamper with infrastructure, such as transportation and government operations (Andress & Winterfeld, 2014). In most cases, these attacks are politically motivated with the intention of forcing a government or a population of people to act in a specific way or to meet demands of the attackers. It further involves illegal access to information from the government for political, military, or economic benefits. Cyber terrorism and warfare, according to national defence leaders, poses a great risk to the national security of the U. S (Brady, 2011).

Cyber terrorism and warfare has three main components. The first component is computer network or the internet. Attackers use the internet to get illegal access into a computer network. The second component is violence and unlike other forms of cyber attacks, cyber terrorism can involve use of violence such as nuclear attacks. The third component is political motivation and rival nations or groups of people seeking political advantages carry out most cyber terrorism and warfare operations (Porterfield, 2011). Although the U. S military department and aviation industry remains relatively secure from these attacks, other sections of the economy are vulnerable to attacks (Reich & Gelbstein, 2012). This has led to increasing fear of cyber attacks among people. Despite these fears, cyber terrorism and warfare remains hypothetical now. There is need, therefore, for increased supervision of terrorist operations on the internet. This will ensure that national security agencies are able to respond immediately when new vulnerabilities are identified (Schiller, 2010).

References

Andress, J. & Winterfeld, S. (2014). Cyber warfare: Techniques, tactics and tools for security practitioners. Waltham, MA: Elsevier.

Brady, A. (2011). A wake up call: Cyber terrorism, cyber warfare & internet terror. Baltimore, MA: Johns Hopkins University.

Porterfield, J. (2011). Careers as a cyberterrorism expert. New York, NY: Rosen Pub.

Reich, P. & Gelbstein, E. (2012). Law, policy, and technology: Cyberterrorism, information warfare, and Internet immobilization. Hershey, PA: Information Science Reference.

Schiller, J. (2010). Cyber attacks & protection: Civilization depends on Internet & email : using research from the Internet. Scotts Valley, CA: CreateSpace.