Good essay about the danger of cyber terror

Sociology, Communication

The aphorism, technology is the capital of human habitation, is thus far true given the developments in information technology. Every single application involves some element of technology with smart and small gadgets that have computer characteristics increasingly finding their application in systems. The application is not limited to any field as it is spread across board in education, transport, energy, industry, trade, among other fields. In other words, the world has become overly reliant on information based technology. This reliance comes with its advantages and costs. The former include increased efficiencies, less costs and less time consumed in the delivery of services. However, the costs include issues of security, safety, immoral considerations, among other factors. This paper shall specifically consider cyber terrorism as one of the threats of increased application of information technology.

Cyber terrorism can be broadly described as attacks on the information technology systems essentially carried out through the internet applications. Cyber terrorism is considered terrorism because of its common strand with terrorism in that like terrorism proper, its main intention is to occasion destruction and losses. For purposes of this paper cyber terrorism activities should be considered as internet applications that are intended to cause among others sabotage, inefficiencies, miscalculations, errors and mistakes. In addition, cyber terrorism is deliberate in that the perpetrators have both the mental intention and the commission or omission intended to occasion the said loss.

Cyber terrorism has been made possible because of the integration of systems through the worldwide web. In the interest of facilitating worldwide

communication and transactions, it has been necessary to network and integrate systems and networks. These include banking networks, communication networks, transport networks and millions of businesses which afford their clients online transactions. Cyber terrorism may be manifested through the attack of such systems. This has been made possible because of the manufacture of viruses and other computer attack weapons. The viruses have, among others, a replicating character in that once accepted into the system, they replicate numerously throughout the interfaces connected to the system. Depending on how the virus is designed, it could occasion a number of activities. For example a bank system virus could go about doubling the bank balances of clients in the account; a school system virus could introduce millions if not thousands of new students while a communication virus could intercept the communication in the system to a preset area.

In efforts to prevent cyber terrorism, organizations have been advised to secure their systems thoroughly, ensure the system is resilient and has the ability to send signals of attempted attacks. In addition, organizations must always have back-up systems that come in handy in cases of sabotage. This perhaps is the cost society has to pay for introducing artificial intelligence to an irresponsible community of persons.

References

Baltzan, P. (2011). Business Driven Information Systems. New York: McGraw-Hill Education.

Stair, R. M., & Reynolds, G. W. (2010). Fundamentals of Information Systems (7th ed.). Boston: Cengage Learning.

Weckert, J. (2009). Computer ethics: Future directions. Ethics and Information Technology, 93-96.