Summary

Technology, Information Technology

Computer Sciences & Information Technology ‘ Cyberterrorism’ Summary By 18 April Summary The articles by Gabriel Weimann and Maura Conway focus on one of the most dangerous and destructive crimes of the modern age – cyber crime. Cyber terrorism is the type of violence than invades the information base of every computers, networks and stored data to misuses the information to the will of the person or group retrieving the data unlawfully. ‘ Cyberterrorism hinges on the widespread use of computers by individuals, private industry and corporations, the military, and the government and its agencies.’ (Ching, 2010) The main focus of the two articles is the spreading of this crime in the recent years and the hype created by the mass media, political and economic forces against the threat of such crime. The lack of trail and reporting of such incidences makes this threat question itself. The articles have clarified the concepts of hacking, hactivism, cracking and their relation with and the comprehensive meaning of the word cyberterrorism.

In my opinion, the increasing use of information technology does make us vulnerable to the cyberterrorism more than ever before. I agree with the writer where he talks about the more unconventional routes adopted by the terrorists for spreading terror because of the anonymity, cost effectiveness and mass destruction capabilities. The book ‘ Black Ice’ also shows the possibilities and realities of the cyberterrorisn and the vulnerabilities of the sectors to these crimes. The biggest fear is the ability of the terrorist to command the data once he gets into the system posing threats at national level. The absence of physical landscape and defying the constraints of the law of nature, cybercrime can be very tricky at times. The various religious

groups fight for their right through the cyber encroachment and the history has also witnessed credit card threats and invasion of bank internet facilities through the cybercriminals. Apart from the above agreements there are few points in the articles where I disagree with the writers. The point that no real cases of cyberterrorism is reported or witnessed, I still believe that the hype is not just for the sake of it. The hype for me is the call of awareness, the information required by the general public in order to foresee what is coming. Although no such incidence has happened the proactive human nature says awareness should be at every doorstep to fight what is as quiet as a snake and more devastating than an earthquake.

In real life, schools and universities can spend a part of their budgets on creating better fire walls for better protection of their data and discouraging the students who eye this glamorous crime by not giving them any means of success. A vigilant analysis of the data setup and monitoring the usage of the internet by the schools, universities and in homes is the need of the time. The students should be explained the difference between the use, misuse and offensive use of the information technology. Creating awareness and abandoning such crime at community level will help us build a generation that would work together in eliminating this crime at the national and international level.

Reference:

Ching, J. (2010). Cyberterrorism. (Ist ed., p. 6). New York: The Rosen Publishing Inc.