Cyber terrorism poses threat to national security

Terrorism has relocated from the traditional world to the cyber world. Terrorism has entered a new age where a combat zone has emerged in cyberspace. The health, wealth and security of nations such as the United States of America is in jeopardy as critical infrastructures are targeted by terrorists through cyberspace to bring terror to the nation. Cyber terrorism has made terrorists to be more vibrant and less suicidal: there is now no need for travelling long distance with explosives, chemical and biological weapons that might put their lives in danger. This research paper aims to outline reasons behind terrorism relocating to cyberspace, how terrorists intend to use cyberspace to bring terror and the advantages that cyberspace has given them.

Traditional tools of terrorism are often regarded as a one step forward and two steps back method as traditional tools are sometimes suicidal and their destination might not be reached. Cyber terrorism is thus a stepping stone for terrorists as they can destroy, hack into systems, alter information and their attacks cannot always be anticipated. Accordingly, this research focuses on how cyber terrorism poses a threat to national security. Based on this threat several aspects of national security espionage will be outlined. Information about economic espionage will be discussed where the economic intelligence is under threat of cyber terrorists. Information warfare will be touched on for example how television and radio transmission can be hijacked and the leakage of sensitive information be used to sabotage stock exchange. Cyber warfare will also be covered to see how cyberspace is used to target the military operations and its facilities.

In conclusion, types of cyber terrorism groups that target national security will be discussed. Statistics on cyber terrorist threats will be looked at and ways to stay safe from those types of threats.

Introduction

Cyber terrorism has been defined in many ways but the main objective is to bring terror by the use of cyberspace. Terrorists have found a comfortable and much safer environment to launch their attacks. Cyberspace has become a training ground, recruitment and training agency, a meeting place and a marketing tool for terrorists. Cyber terrorism causes great discomfort to national security as terrorist organisations, foreign governments, criminal organisations and individual hackers develop new ways to attack critical infrastructures, the military and the government.

Cyber terrorism tools has made cyberspace to be the head-quarters for terrorists. Cyber terrorism has become the new weapon of mass destruction for terrorists where their cyber attacks may go unnoticed or at the time of notice, the response time may be limited. Cyber terrorism has given terrorist reason of attacking national security at any given as cyberspace is more advantageous than traditional methods.

National security is said to be the requirement to maintain the survival of the nation-state through the use of economic, military and political power. The greater the capacity national security has of holding sensitive information and trade secrets, the greater the capacity to feel pain from cyber terrorists. Now the national security needs to protect the survival of the nation state and also its survival from terrorist’s attacks. Since well national security cannot fight cyber terrorism on its own they are agencies such as the National Security Agencies (NSA), the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) which help national security fight cyber terrorism.

Cyber terrorism if not challenged head on will cause great deal of damaged terrorists relocated to cyberspace after seeing an opportunity that military power in not that dominant in cyberspace. In cyberspace terrorists have privileges of launching an attack at any time with no fear or doubt that it might not succeed or reach the designated area. Cyber terrorism is a trial and error method if the attack did not succeed u can try again mot like traditional method where as if u failed its either you die or end up in jail.

Cyber terrorism takes many forms. One of the more popular is to target national security which is taken to be national security espionage. National security espionage ranges from economic espionage to information warfare and cyber warfare.

Cyber terrorism stats show that every year enormous amount of money is lost due to cyber terrorism, cyber terrorists target critical infrastructures for making money or they fundraise in cyberspace to raise funds for attacks. Cyberspace has given terrorists a free way of launching their attacks we may fare for the worst as everyday terrorists manage to recruit and train its own army of terrorists the various number of available cyber terrorism tools has to the level of terrorism to an advanced level. We may ask ourselves if the world will ever be ready for a full length cyber terrorism attack. Where will the attack hit and will it be detected in time to respond to the attack?

Background

Cyberspace has become a combat zone

The relocation of cyber terrorists from traditional tools to cyberspace has established a much safer and comfortable environment for terrorists to launch their attacks. In the process their relocation has triggered a robust and dangerous war, this war if fought between national security and cyber terrorists.

The battleground has being set in cyberspace, Nation states have created cyber-warfare units, this unit will be known as USCYBERCOMM which is headed by Keith Alexander. Richard Clark said at the RSA conference China and Russia are stealing petabytes of information he also said that the government of China and Russia are successfully engaging in daily activities of stealing anything worth stealing and the United State government and private industry are not stopping them. Terrorists seek to harm the survival of the nation, harm the economy and target critical infrastructures of regions they are targeting. The survival of the national security might be left in shambles if a full scaled cyber attack may be launched against them. Although terrorists have not successfully launched a substantial cyber attack, the threat is there and grows bigger and bigger with every small cyber terrorism attack. With this small cyber attacks, cyber terrorists are gaining more experts and experience. A question may come to mind why are terrorists launching these weak attacks? What is the bigger picture that they are trying to painting? Will the answer to this question be that they are trying to find loop holes in systems to be targeted? We will never know until that time comes.

National security depends on military power for security but the military is not dominant in cyberspace as it is dominant on surface land and in the sea. Military have limited resources to take on cyber terrorism. Terrorists seek to attack through cyberspace where their attacks have the potential to reach the destination originally targeted simply because the line of defence is not that powerful. Cyber attacks cannot be anticipated, they are no radars to track incoming attacks in cyberspace.

Targeting critical infrastructures

The move of terrorists to cyberspace has left the world in shivers as the world depends on critical infrastructures for survival and making earns meat. Targeting national security will reduce the ability of protecting the nation; if the ability of protecting the world is reduced terrorists can strike in ways that we cannot image. People are not safe in their homes as gas pipelines pass under their houses cyber terrorists can cause a major gas pipe line burst of regions they are targeting the terror of September they 11 may be relived with the use of pipelines this time.

Advantages of cyber terrorism

Cyber terrorism is much safer than traditional tools; cyber terrorism has made terrorists to be lee suicidal.

Terrorists can cause greater damage at less risk of being caught in the crossfire.

Recruitment, teaching and fundraising is simple, they can recruit people make a lot of money in a short space of time.

They is no need for terrorists to travel long distance with biological weapons and bombs, attacks can be made remotely from anywhere in the world.

Their attacks cannot be anticipated can cause great impact.

No check points to go through for terrorists to reach their destination.

Cyber terrorism is cheaper than traditional methods.

National security espionage

National security espionage can be defined as the use of cyberspace by terrorists to penetrate national security systems to try and steal critical information, trade and government secrets and target critical infrastructures. National security protects the nation through the use of economic, military and political power. Cyber terrorists seek to exploit the fact that national security holds sensitive and dangerous information which can harm the survival of national security and the well being of the nations. National security espionage can take many forms which ranges from economic espionage to information warfare and cyber warfare here is an overview of the three types of national security espionage which are mentioned above:

Economic espionage

Economic espionage also known as industrial espionage is known as the use of cyberspace by under developed countries, commercial or industrial enterprises to gain information of trade secrets which are not available on open channels. Cyber terrorists target Europe and the United States of America as they posses’ power in the market areas, they have top companies and they are fully developed.

Types of cyber terrorism groups that cause terror to national security

They are various types of cyber terrorism groups, but the one which cause great deal of panic is those that target national security being for political purpose, industrial espionage or cyber warfare. Whatever the target may be towards national security, the outcome of the attack will be enormous. Groups like:

The Osama bin Laden Crew – This is a group of cyber jihadists which was found in the year 2000 by Abdullah Quraischi.

Al-Qaeda

Cyber terrorism tools and techniques

The biggest tool for terrorists has become the internet. The internet is an immeasurable digital library, anything about any organisation can be found in the internet. Terrorists use various tools in cyberspace to bring harm, they use tools like:

Distribution Denial of Service (DDoS)

This is an attempt of denying services, making computer resources not to be available to the intended users.

Sniffers

Sniffers are used to get passwords of systems (spying of passwords).

Rootkits(Musk intrusion)

Rootkits are utilities installed in a victim’s machine to ensure that a cracked system remains available to the intruder. Rootkits are difficult to trace as the system will work as its being working before.

Network Analyzers (SATAN)

Spoofing (smurfing)

Worms

Worms are programs which makes copies of itself and copies to other computers trough out the network.

Trojan Horses

Is the software program which runs on the victims machine and can run secretively

BackDoor

Backdoors allows hackers to enter systems again at a later stage without being noticed

Botnet (zombie army)

Botnets are malicious software’s which runs automatically on computers which are hacked.