International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 09 , September 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

CYBER-TERRORISM A THREAT TO GLOBAL SECURITY

Kirandeep Kaur[1], Suket Arora[2]

[1,2]Department of Computer Applications

[1,2]Amritsar College of Engineering & Technology, Manawala, Amritsar, Punjab, (India)

ABSTRACT

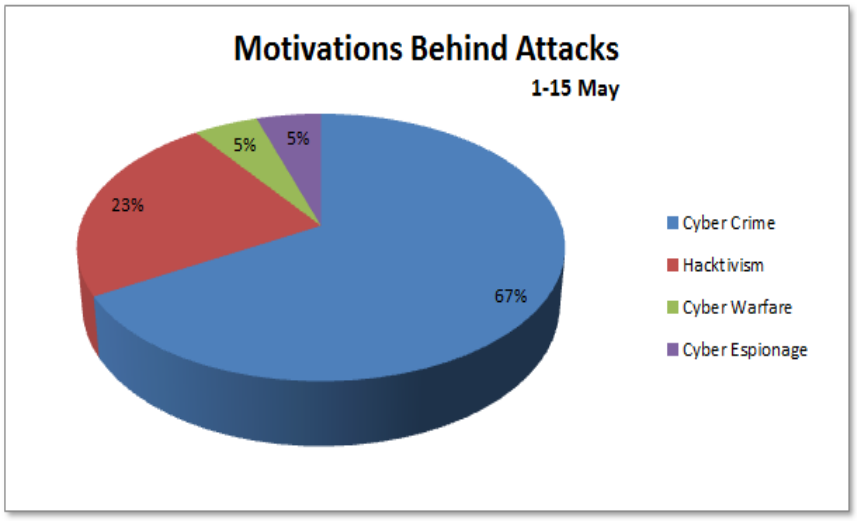
The current era has seen more rapid and extensive change than any time in human history. The profusion of information and the explosion of information technology is the driver, reshaping all aspects of social, political, cultural and economic life. The effects of the information revolution are particularly profound in the realm of national security strategy. They are creating new opportunities for those who master them. The purpose of this paper is to explore how the Internet is altering the landscape of political discourse and advocacy with particular emphasis on how it is used by those wishing to influence the cyber security. Emphasis is on actions taken by non-state actors, including both individuals and organizations that how the intruders harm the policy decisions triggered by the Internet. [4]The primary sources used in the analysis are news reports of incidents and events. The goal of this article is to provide a new explanatory angle concerning the possible targets of terrorists' offensive information warfare (OIW) operations. In this paper we will review the types of cyber-terrorism, from the internet as a platform for propaganda to actual cyber-attacks and the preventative measures and information security available, as well as the social ramifications of a more regulated internet.

Keywords: Crime, Attacks, Cyber Attack, Cyber Terrorism, Threat

I. INTRODUCTION

Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb. [2]—National Research Council Cyber-terrorism is the convergence of terrorism and cyberspace. [1] It is generally understood to mean unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate a government or its people in furtherance of political or social objectives. Further, to qualify as cyber-terrorism, an attack should result in violence against person or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact. The main problem with these virtual attacks is that these are not caught up red-handed most of the time. The reason can be the fast growing technology that intruders are smart enough than other engineers. More and more, everyday facts of life are being integrated digitally and as our nation's infrastructure becomes linked, it also becomes more vulnerable. The opinions of cyber-terrorism's existence and possibilities are far ranging, from those who believe that it's not really a threat and could never do any serious or lasting damage.

International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 09 , September 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346



II. THE NEW TERRORISM

[6] The biggest fear of many people and government agencies, however, is the threat of an actual cyber-attack. In this modern age, everything is being networked, and many systems are reliant on computers and on computer networks. Hackers and viruses have always been a very real threat that we have dealt with in the past, causing disruption and spreading fear. Imagine the damage that could be caused if vital infrastructures or sensitive computer networks' security were breached. Disruption via cyber-attack could be caused to a variety of communication systems, including internet, phone, and cable. There is the possibility of breach into secure networks responsible for running corporations, hospitals, or even government agencies. Telecommunications networks and electrical power grids, even banks and economic systems could be disrupted by determined cyber-terrorist hackers. Such attacks could cause widespread panic, and even do damage to the economy. Various operations and tests have been carried out in the past to determine the security of various military installations and critical computer networks.

III. COMPONENTS

Some research is shared in order to elaborate the discussion on cyber-terrorism. These include:

3.1 Case study on Cyber-terrorism

3.2 Response to Cyber-terrorism

3.3 Future of Cyber-terrorism

3.1 Case study on Cyber-terrorism

Terrorists have even been known to use normal websites such as various social networking sites like Myspace, Facebook and even Youtube to spread their propaganda and threats. Most well known are the actual videos and stills of terrorist acts that have been posted on the internet, including beheadings, shootings and other acts of violence and terror. The nature of the internet makes it the ideal forum to spread these acts; Being quick to spread, hard to shut down, and very difficult to trace. [6]

One very well known terrorist group make use of the internet for their purposes is Al Qaeda's cyber-propaganda. Al Qaeda has used the internet to post claims of responsibility for various acts, such as the downing of Kenyan airplane, and the bombing of the Jakarta Marriott Hotel on 5 August, 2003. They also use

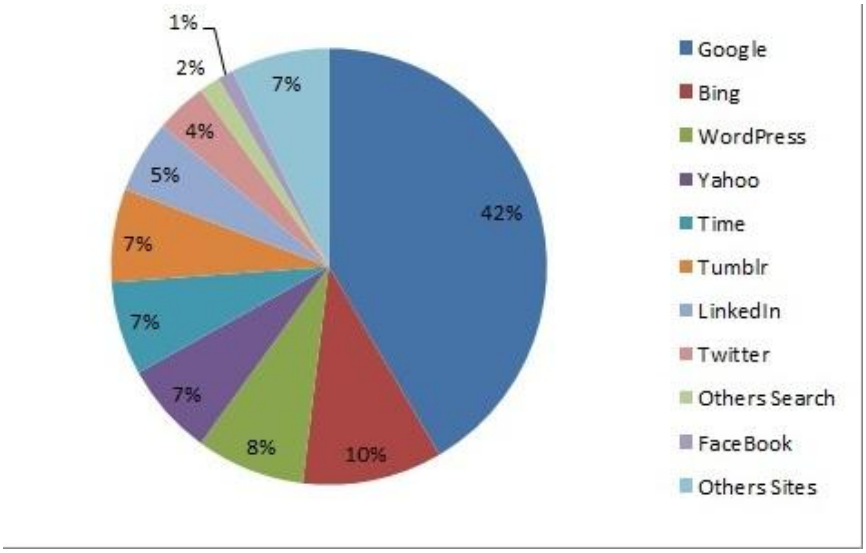
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

the web site al Qaeda's Center for Islamic Studies and Research, which published the online journals Sawt al-Jihad, and The Voice of Jihad. These online magazines focus on the use of violence as jihad's only way and their support to help spread their messages. [6]

In January of 2003, the SQL "Slammer" virus rendered 13,000 ATMs Bank of America. ATM machines inoperable and forced Continental Airlines in New Jersey to ground flights due to system inoperability. [6]

In 1998 a 12-year old hacker broke into the computer system controlling Arizona's Roosevelt Dam's floodgates and had complete control over the system, which would have allowed him to flood the city of Phoenix. [6]

More recently is the Stuxnet computer worm, which was discovered in July 2010. This Windows based worm targets industrial software and equipment, and was the first malware discovered that spies on and subverts industrial systems. The worm included a highly specialized malware program that targeted Siemens Supervisory Control And Data Acquisition (SCADA) systems. Although the worm infected many computers, it only did damage to the Iran nuclear program Siemens SCADA system. It specifically targeted the centrifuges used in the production of nuclear material, making them spin so fast that they were damaged. The worm even covered the change in speed to prevent it from being discovered. This went on for a year before it was discovered and the damage it caused to the Iranian nuclear production plant is estimated to have set back the program about two years. [1]



3.2 Response to Cyber-terrorism [1]

In 1996 President Bill Clinton issued Executive Order #13010, which dealt with the protection of critical infrastructure. It mentioned "threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats")" (http://www.fas.org/irp/offdocs/eo13010.htm) It was a basic plan to deal with threats to critical infrastructure and outlined the agencies that were part of this plan. Mainly, the objective was to protect institutions and have plans for their continued operations.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Once again in May 1998 the issue of cyber security was addressed in the Presidential Decision Directive 63. This directive was aimed at protecting the critical infrastructure. It summarized the need to address vulnerabilities. It also put the burden on the Federal Government and its agencies to get involved and stressed public/private partnerships. President Clinton stated his intentions to "take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems." (http://www.fas.org/irp/offdocs/pdd/pdd-63.htm)

In February of 2003 the White House released The National Strategy to Secure Cyberspace. This report is "a 76-page document outlining a sustained, multi-faceted approach to safeguarding the nation's vital communications technologies." (http://usinfo.state.gov/journals/itgic/1103/ijge/gj11.htm) It acknowledged the importance of the use of computer networks and their security in maintaining National Security. The plan outlines the need for a planned response to cyber attacks as well as preparedness and prevention methods. In President Bush's letter addressing Americans in the document he describes it as "a framework for protecting this infrastructure that is essential to our economy, security, and way of life." (United States, 2003.)

The strategy itself is made up of five key points which are:

1. a national cyberspace security response system;
2. a national cyberspace security threat and vulnerability reduction program;
3. a national cyberspace security awareness and training program;
4. securing govenments' cyberspace;
5. National security and international cyberspace security cooperation." (United States, 2003. Pg 54)

The plan addresses particular safeguards and the role of federal, state and local government agencies. Overall, the United States has made it clear that there are concerns for protecting America's critical infrastructure and securing cyberspace. Efforts have been made to address these concerns and to clearly define whose responsibility it is to do so. In moving forward it is important for our country to continue to identify new threats and respond to them with solutions.

3.3 The Future of Cyber-terrorism [1]

In moving forward in the age of technology it would be foolish to discount the risks of cyberterrorism. It is important to keep in mind that "the next generation of terrorists are now growing up in a digital world, one in which hacking tools are sure to become more powerful, simpler to use, and easier to access." (Weimann, 2006. Pg 170) If you consider how easy it is to attain the tools and skills necessary to carry out an attack you then must consider the true threat that cyber-terrorism posses to our National Security. Knowing the intent of terrorists opens up many possibilities of using technology to achieve their goals. Consequently, "in the future, the logic bomb rather than the conventional bomb may prove to be the terrorist weapon of choice." (Hodge, 1999. Pg 105)

It is expected that "in the future, the threat of cyber-terrorism appears more ominous… cyber-terrorists have the advantage of attacking from almost anywhere, by themselves, at a minimal expense, without risk of harm, and with limited risk of detection." (Purpura, 2007. Pg 61) Many experts believe that this is a real threat and must be dealt with. As suggested by Barry Collins, Senior Research Fellow at the Institute for Security and

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Intelligence, "cyber-terrorism… is a misnomer in that the consequences are not limited to the world of cyberspace but occur in the physical world." (Hodge, 1999. Pg 105) He goes on to say that "if we fail to be ready when and where the virtual and physical worlds converge, then all that will be left is terror." (http://afgen.com/terrorism1.html)

Historically, terrorism has been characterized by acts of violence carried out with the intent to cause panic and fear. But with cyberterrorism "the face of terrorism is changing. While the motivations remain the same, we are now facing new and unfamiliar weapons." (http://afgen.com/terrorism1.html) Frank Cilluffo of the Office of Homeland Security stated "while bin Laden may have his finger on the trigger, his grandchildren may have their fingers on the computer mouse." (Weimann, 2006. Pg 170) The emerging threat of cyberterrorism is quickly growing and becoming a reality. We can no longer sit idly and disregard the possibility of a cyber attack. It is "likely that the threat will increase in the future for a coordinated cyberattack… cyberterrorism become increasingly more mainstream in the future." (Wilson, 2005. Pg 22) If we fail to prepare for this inevitable future we allow terrorists an avenue to accomplish their goals.

There should be counter-cyber-terrorism standards in place for such activity. Our preparedness and response to an attack should be planned. We need to be able to detect and then recover from any attempt at illegally accessing a computer network. A successful reactive strategy "will detect and respond to Internet events… and coordinate cybersecurity and incident response with federal, state, local, private sector and international partners." (http://www.pcworld.com/article/111066/homeland_security_to_oversee_cybersecurity.html)

IV. PREVENTATIVE MEASURES

Efforts need to be undertaken and precautionary measures put in place. [1]A strategy for cyber-terrorism should be two- fold: First, a proactive approach that anticipates future events and attempts to avoid them. The best way to deal with an attack is to be prepared and prevent it from happening in the first place.

Secondly, a reactive approach which deals with the response to a cyber-terrorism event. This involves identifying and reacting to an attack. We must locate our vulnerabilities and harden them before they are exploited.

Critical infrastructure needs to be secured as well as the computer networks that control them. The need for secure computer networks does not only apply to government agencies but also to private sector companies that have databases of crucial information. Unlawful access to these networks could be catastrophic. A proactive strategy needs to be updated regularly and be one step ahead of those it is designed to protect against. Continuing safeguard measures needs to be explored in order to seriously address the invisible threat against the United States.

Coming to some preventative measures: Firewalls and anti-virus programs are always being worked on, made to be tougher and quicker at virus detection. Operating systems security has been made stronger.

[6]Another method of security is through the monitoring of the internet. Searching social websites, suspected terrorist web-pages, and even online communications such as chat-rooms and E-mails, is used to detect terrorist activity or terrorist threats. This process is called sniffing. A sniffer is a software program that searches internet traffic for specific items or keywords it's programmed to find.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[6]Many people are in protest to such invasive programs, such as the Magic Lantern technology, being developed by the FBI, which allows investigators to secretly install eavesdropping software onto a person's computer and record every single keystroke.

V. TECHNIQUES

This research was conducted using open source documents that are open to the public. All documents are unclassified and openly available for viewing. References used for the analysis of the topic were found via the Internet. Examples of works cited are unclassified government documents found on government websites using search terms related to the topic. Internationally distributed newspapers were also used to support the construction of the paper. Other valid and reliable sources used in collecting data were government websites for agencies such as the Federal Bureau of Investigations (FBI). Furthermore, books written by experts were examined and relevant information was extracted to reinforce the views within this text. A logical analysis of the material was conducted and presented in this paper.

VI. CONCLUSION

It is important, to always have up to date patches for security, and for the developers to provide new patches against new threats as quickly as possible. In these regards, constant vigilance is important. There is no such thing as perfect security, and we must always work to make sure our systems are as safe as possible.

Overall, the future of cyberterrorism and the role it plays is somewhat unknown. But what is known is that the threat exists and it is real. We must take several measures to safeguard against cyber-terrorism. There are documented events of cyberterrorism and how terrorists use cyberspace to conduct their business. Additionally, the threat to our critical infrastructure is far too serious to be taken lightly. The threat of cyberterrorism has been addressed by several presidents and acknowledged by many reputable professionals. The government has also played a role by drafting numerous Executive Orders and Presidential Directives. But it seems these efforts to assess and manage the threat fall short. More steps need to be taken for awareness and incident response and they need to be taken now. If we continue to question whether this threat is viable and do nothing about it, we are vulnerable to an attack. Ultimately "the threat of cyber terrorism may be exaggerated and manipulated, but we can neither deny it nor dare to ignore it." (Weimann, 2004).

REFERENCES

[1] https://articles.forensicfocus.com/2012/06/01/the-role-of-cyber-terrorism-in-the-future/

[2] https://www.princeton.edu/~ppns/Docs/State%20Security/Cyberterrorism%20-%20sum%20of%20all%20fears.pdf

[3] http://eprints.ugd.edu.mk/6849/1/CYBER%20TERRORISM%E2%80%93%20GLOBAL%20SECURITY%20THREAT%20-%20Mitko%20Bogdanoski.pdf

[4] http://www.nato.int/structur/library/bibref/cyberterrorism.pdf

[5] https://www.symantec.com/avcenter/reference/cyberterrorism.pdf

[6] http://cyber-terrorismpaper.blogspot.in/