Cyber Terrorism - An International Phenomena and An Eminent Threat

Biny Pal Singh*
Ankit Verma**

Abstract

This paper goes into the conception of terrorism, who the terrorists are and tries to establish a grasp of why they conduct the activities they do. Understanding the attacker will allow recognize the type of attack they may plan and the aftereffect they are likely to try and accomplish. It looks at the main encouragement of Terrorist groups and considers their use of the Internet for various forms of a terrorist Campaign such as implantation/advertising and recruitment. It will acknowledge the various channels that have been used and how the Internet has provided a new liberty for terrorists to conduct their campaigns and how it has been adapted by them for their purposes. It examines the probable threat of a cyber-attack by terrorist organizations and how they can use the Internet and Cyber Space to their liberty and attack a target with similar results to a conventional physical attack. The paper will briefly examine some of the possible defenses against this form of terrorism.

Keywords: Terrorism, Terrorist encouragement, Cyber-attack, Terrorist use of the Internet

Introduction

If 10 security experts who create various forms of protection against 'cyber terrorism' are asked what 'cyber terrorism' is, you will get at least nine different definitions! When those 10 experts are in the field of computer security, this discrepancy moves from comedic to rather worth consideration and serious. When these 10 experts represent varied departments of the governmental agencies tasked with protecting the infrastructure, defense and assets of our nation, it becomes a critical issue. However, given the lack of scientific groundwork/platform to incorporate various aspects of computer-related crime into the category 'cyber terrorism', this situation should not be surprising.

Understanding Terrorism

Most people who are asked about terrorism would say that they know who terrorist are and what terrorism is, but surprisingly there has never been internationally agreed definition. but considering violence or threat of violence as theme there have been literally hundreds of definitions that have tried to throw light on this international phenomena. The only other elements to appear in more than 50% of definitions are "Political" and "Fear, terror emphasized" [2]. Terrorism dose differ from other crimes in its core; it is done with a purpose in mind and an aftereffect that is expected from its occurrence. Considering who the terrorist are is most important. Considering size and ability there are literary hundreds of terrorist groups, which to some extent, warrant the label of terrorist. Terrorism has 4 classic encouragements [3].Firstly there are terrorist with single issue, those who have faith in one particular cause and are ready to use violence to protect their message in the faith of ending the issue. Although commonly small and at less devastating rate, these groups can use the cyber world to their aid as in cyber environment they can effectively push forward there cause and end the issue with very less lethality rate. The terrorist who use violence to effectively promote their political ideology are the ideological terrorist. Religio-political terrorist groups are more dangerous as there believe is that they are acting for GOD himself or on a spiritual order and that those not of their belief

Biny Pal Singh*
Student (BCA)
IITM, Janak Puri, New Delhi-110058

Ankit Verma**
Assistant Professor
IITM, Janak Puri, New Delhi-110058

are against GOD [3]. There are extremist groups spanning all major religions and some minor cults who have resorted to terrorism. These terrorist have acted outside their religion and abused it, they misrepresent their religion in their claims and must not be confused. Although warfare and violence have been circumstantially justified in many religions, none, with the exception of a doomsday cult such as Aum Shinrikyo, would apply this as indiscriminate targeting of security forces or civilians outside the legal borders of warfare. The Groups who evolve there motivation or have heterogeneous aims can be hybrid terrorist groups, as with any definition of labeling model. The Provisional IRA are an example, they were a Nationalist group as they wanted Northern Ireland to cede from the United Kingdom to the Irish Republic but were also an Ideological group as they wanted Ireland to become a Socialist state. Considering the terrorist themselves, consideration on their psychology is important to get to the point where we can understand how to defeat them. Terrorist don't have a clear profile, they come from all aspects of life and have varying motivation, educational, employment and wealth. That all not being mentally unstable is the only common factor among them all as, terrorist organizations want the ability to think and reliability to exist among all of its activists. The role of the terrorist be decided on their intelligence level and also by any specialist skills such as chemistry or IT. And there must be a requirement for college level members as well they have more basic standard of education. It must be accepted that most of these terrorist groups are comprised of skilled and exceptionally-intelligent people who are acting out of genuine belief (self-formed, independent) and not a group of clueless idiots. Cyber defense plan against terrorism must consider this; they will study, take time, make plans and hire experts of the highest caliber to achieve their aim.

Hacking Techniques – Types of Attacks

According to Galley's discussions from 1996 there are three types of attacks against computer systems:

- Physical
- Syntactic
- Semantic.

Conventional weapons are used in a physical attack, such as bombs or fire. Where as to disrupt or damage a computer system or network a syntactic attack uses virus-type software a semantic attack can be taken as a more subtle approach. It attacks users' confidence which is done by causing a computer system to produce errors and results which are unpredictable. Syntactic attacks are categorized under the term "malicious software" or "malware". The use of viruses, worms,

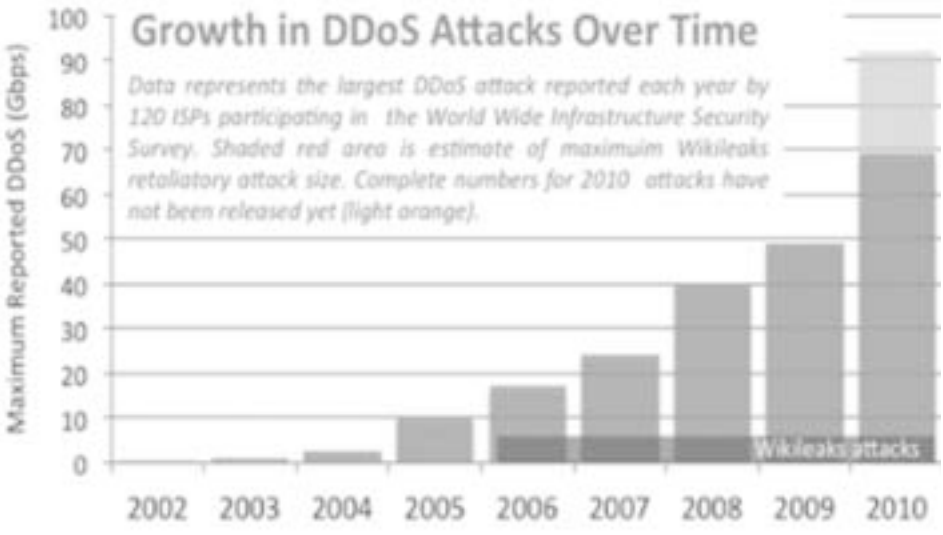

Figure 1: Growth In DDoS Attacks From 2002 Till 2010.

and Trojan horses is done in these types of attacks. Email is one of the most common vehicles of delivery for such malware. Denial of service (DOS) and distributed denial of service (DDOS) attacks are also included in Syntactic attacks. In recent years attacks such as these have become more widespread. Ping saturation is one of the most common technique forms of DOS and DDOS (Vatis, 2001). Ping is an Internet utility used commonly to verify that a device is available at a given Internet address. Ping saturation occurs when ping is used in an attack to overwhelm a system. The intent in these types of attacks is to disrupt services on a network or system by flooding it with requests. Modification of information or dissemination of incorrect information is involved in Semantic attacks (Schneider, 2000). Even without the aid of computers, Modification of information has been perpetrated, but new opportunities to achieve this have been provided by computers and networks. Also, mechanisms such as email, message boards, and websites help in dissemination of incorrect information to large numbers of people.

Pure Cyber-Terrorism

Pure terrorism is a category that consists of all those terrorism activities are carried out totally (entirely/ primarily) in the virtual world and have a drastic aftereffect. There are some many ways over the internet where one can meet like-minded individuals in a (comparatively) safely and share information and on a secure line which are used by these terrorist organizations to maintain a contact. No further prerequisite rather than knowledge is required for a successful cyber terrorism event. Knowledge is something that is essentially free to the owner once acquired, and an asset that can be used over and over again. Further, such environment could be facilitating the creation of an entirely new terrorism group. There won't be requirement of any head or chief and the member could organize themselves quickly and easily through cyber-space that could be a threat to the global security and the counter terrorism department itself. This is very different from some examples given above, where the cyber space could aid the activities terrorists, but the real resources are still required for execution of the real plan. The Danger possessed by the cyber terrorists and the significant barrier of our ability to protect ourselves is what writer's means when they toss around pure cyber-terrorism. There is always one question that has never been appropriately addressed in the literature is that what this terrorism might look like. There is a large amount of confusion at this time because of the lack of agreement in an international and intellectual definition for the above question.

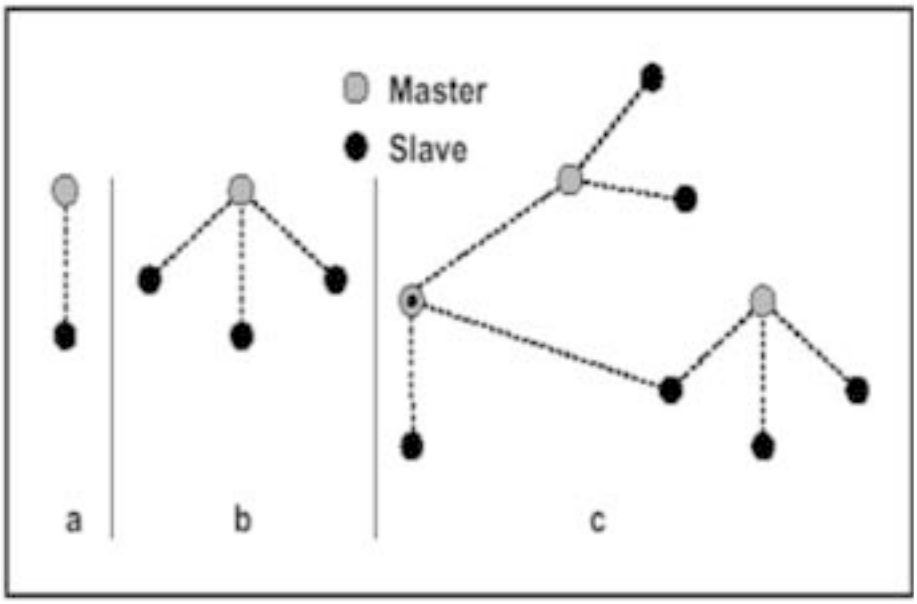

Figure 2: The encounter of Cyber-Terrorist activities in U.S.A and china Cyber-Space

Increase in Cyber-Terrorist Activities

Figure 2 shows that how the cyber terrorism has been increasing its activities and has made the world feel its presence in last 7 years. Till 2007 these activities had seen an increase of 32% and shows that in future it can be an international phenomena and affect every corporate and government of this world.

Computer Weapon of Cyber Terrorism

Following on from the foundation above, the most obvious and curtail weapon of this eminent threat of global cyber terrorism is the 'computer'. So, the question arises that are we purposing that we should restrict the use of a computer on all bases, just as the access to explosives and radio-active stuff is restricted? Not quite it, but close. We mean that the Heap of connected computers needs to be protected. May laws define how one should protect and ensure the security of firearms from illegal/Dangerous use like the gun can fall in wrong hands and can pose danger which is secured by the mandatory use of trigger lock and the RDX explosive material is not sold over the shop at the corner of the street? Computer is certainly not entirely equivalent to explosives or a gun. Thus, a wide number of laws are already present in current system of judiciary that discusses damage done to/by the third party by the intentional/unintentional misuse of corporate/personal piece of information/property/data. The definition of 'misuse' in these laws and there application is unclear till date. However, these laws and standards need to be more clear which will require the operators of large network of interconnected computers take forward appropriate steps to keep these systems safe.

Conclusion

The Development if the internet was done primarily as an open architecture which was unregulated. We are not only witnessing the backlash to the 'corporatization' of the network, Where the Equipment for drastic destruction can be easily be placed in the hands of backward and mindless people, We must also deal with the fact that this infrastructure was/is ideally suited for criminal activities on a wider base. Some of these activities are being promoted as cyber-terrorism. The government and the corporate organizations security is at the risk who are not capable of defending themselves from this eminent threat. Events can are to analyzed in terms of their critical factors that may exist can legitimately be called terrorism. However, if all these factors don't exist then it doesn't means that the corporations are safe. Unfortunately, the structure of corporation are built around the premises that people will do right thing. But as we have seen this is not necessarily the case. We do not use the term 'chemical terrorism' to define bombing of chemical factories, nor will we use it to define terrorism carried out with chemical. Thus, the question arises why the term cyber-terrorism is used to describe any sort of threat or criminal activity carried out with or against computer in general. At the same time, there are some who insist on treating "Pure Cyber-terrorism" as Cyber terrorism who are completely missing the true threat that the addition of acts in the virtual world to the terrorist playbook possess. Finally, the cyber-terrorism has to be given attention separately and cannot be mugged with common terrorism. This artificial fragmentation of our defense System is an advantage for the enemy and is to be avoided at all cost. This brings us to the final Point of this ongoing study: turning the tables on terrorism. As we have seen, computer can play an enormous role in terrorism. But they are also our biggest defense against terrorism its self if used to our advantage, this begins when we re-examine basic beliefs about cyber-terrorism which must take place in industries, academia, government and defense sectors. Analysis of the information must be shared at each level, collated and redistributed across the states, local government boundaries, industries, academia, and in some cases to the citizens as well. The lack of consideration of cyber-terrorism and the overall insecurity of the networks of the World Have allowed a situation to develop which is not best for the country or the computer user. The computing resources are to be protected, and the job of these terrorists is to be made difficult which can be accomplished by only re-examining the commonly held believes about the very nature of the computer system and its counterpart cyber-terrorism.

References

1. Record, Jeffery: Bounding the Global War on Terrorism, Strategic Studies Institute, US Army War College, Leavenworth, 2003.
2. Schmid, Alex and Jongmans, Albert et al: Political Terrorism: A new guide to Action, Authors, Concepts, Data Bases, Theories and Literature, Transaction Books, New Brunswick, 1988.
3. CSTPV St Andrew's University Certificate in Terrorism Studies.
4. COE DAT Information Collation Managemant Cell database.
5. Weimann, Gabriel: Terror on the Internet, USIP, Washington DC, 2006.
6. Weimann, Gabriel: WWW.AL-QAEDA: The reliance of Al-Qaeda on the Internet7.
7. COE DAT Cyber Terrorism Couse IV Mar 09.
8. COE DAT Strategic Communications Workshop May 09.
9. Huizing, Harry: Cyber Terrorism Briefing Note, COE DAT, Ankara, 2008.
10. Krone, Troy: Gaps in cyberspace can leave us vulnerable, Platypus Magazine (edition 90, Mar 2006).
11. COE DAT Cyber Terrorism Workshop Oct 07.
12. Bunker, Robert J: Networks, Terrorism and Global Insurgency, Routledge, Abingdon, 2005.
13. Hennessy, Joh L and others: Information Technology for Counterterrorism, National Academies Press, Washington DC, 2003.
14. Hoffman, Bruce: Inside Terrorism, Columbia University Press, New York, 2006.
15. Huntington, Samuel: The Clash of Civilizations, Free Press, London, 2002.
16. Laqueur, Walter: The New Terrorism: Fanaticism and the Arms of Mass Destruction, Oxford University Press, New York, 1999.
17. Sageman, Marc: Understanding Terror Networks, Penn, Philadelphia, 2004.
18. Stern, Jessica: The Ultimate Terrorist, Harvard University Press, Cambridge MA, 1999.
19. Tuman, Joseph S: Communicating Terror, Sage, Thousand Oaks, 2003.
20. Whittaker, David (ed): The Terrorism Reader 3rd Ed, Routledge, London, 2007.
21. Wilkinson, Paul: Terrorism versus Democracy, Routledge, London, 2006.