Cyber-Terrorism: Hype or Hazard?

Shuaib Zahda – January 2010 – email: shuaib.zahda@gmail.com

Bombing, hijacking airplanes, haphazardly shooting innocent people, 9/11, and many others are phrases and expressions associated with terrorism. Nowadays, terrorism has been attached to the cyberspace. Never before has anybody thought that terrorism would have a digital form. Indeed, the Internet is a double-edged sword, one edge is assisting humanity develop and advance rapidly, and the other is adversely affecting it. Regardless of the hype cyber-terrorism is a real threat in this global and open-minded era. It will lead to global conflicts if not confronted head-on by governments worldwide working in unison.

Cyber-terrorism is an international phenomenon which must be combated by the international community. Some collaboration against cyber-crimes exists but it is on a limited scale. For example, in 2007, Estonian governmental computer systems have been targeted and disrupted by Distributed Denial of Service attacks (DDoS) using “botnets” wherein, thousands of computers participated without their owners’ knowledge about the attack. It crippled most of the state Internet services and caused inconveniences amongst the Estonians. Consequently, the Estonian government asked the NATO and the USA cyber-experts help and it resulted in recovering the systems and determining the origin of the attack which was from Russia. This proves that international cooperation is effective.

Moreover, there is an urgent need to keep the international law up-to-date since the technology is advancing faster than the laws. The current international law is inadequate for addressing and tackling issues in cyberspace. Even many countries’ legislations do not have computer related laws. For instance, in 2000, the “I LOVE YOU” worm which affected tens of millions of computers worldwide causing an estimated $5.5 billion damage was made by a Filipino student. He was released and all the charges against him were dropped because there were no laws against proliferating malware at that time in the Philippines (2).

Never has the law by itself been sufficient without strong enforcement by states or the international community. Since the Internet is borderless, and cyber-attacks are asymmetric, remote and hidden in nature, it is a necessity that equally borderless organizations combat cyber-terrorism, since it is not a matter of a any individual country. However, several countries might be affected by an attack. In the case of the “I LOVE YOU” worm creator, he should have been admitted to the international court and been sentenced
there, since his crime not only affected the Filipinos but also peoples and governments all over the world. Furthermore, the need for cyber-crime deterrence has become more essential than ever. Indeed, hackers easily attack their targets anonymously from several locations in the world simultaneously, which makes it very difficult to one nation to trace and respond to such attacks on its own. And, old illicit cyber-activities such as stealing personal information, and intercepting messages, for example the “intercepting live video feeds from U.S. Predator drones”(6). Along with the existing attacks, as technology advances, cyber-crimes will take new shapes and dimensions and will become more sophisticated.

Many governments are fighting cyber-terrorism and seriously considering it as a part of terrorism. Ministries of Defense from around the world have been setting up new cyber-deterrence divisions. In 2008, “President George W. Bush signed two presidential directives calling for the creation of a comprehensive national cyber-security initiative” (5). Followed by the current USA President Obama who called cyber-security “one of the most serious economic and national security challenges we face as a nation”(4). Despite the increase in anti-cyber-crime is some states, no single state can be effective against cyber-crime if they act on their own.

Nowadays, cyber-war is used in conjunction with conventional war. To illustrate, in the last Gaza-Israeli war thousands of Arabic and Israeli websites were defaced, ”Hackers involved allegedly included members of the Israeli Defense Forces and Hamas, which makes this one of the few cyber-events which involved official State involvement“(1). Besides, cyber-attacks were also used by the opposition protesters in the latest Iranian presidential election, “One of the forms of protest was the use of DDoS attacks directed against Iranian government Websites using the popular social software service Twitter as an organizing platform“(1).

Besides, countries must have solid policies and proper response strategies to cyber-terrorism. It is a direct threat to the economy, and it can be as serious as shutting down the electricity of a region for several days. As a result, major portion of the economic activities in that region would be paralyzed. According to Bruno: “if you can do that with a pure cyber-attack on only one critical infrastructure, why would you bother with any traditional military attack” (5). So, cyber-weapons are available to all people and can be easily used against any infrastructure.

However, many analysts and experts claim that cyber-terrorism and cyber-war are hypes and the propagandas have been spread by security companies for commercial benefits. According to Morozov:
“DDoS threats have been far more commercial than political. The driving force has been cyber-gangs ... which are in the extortion business” (4). Despite these claims security companies are an important tool in defense against cyber-crime.

Security companies have been assisting governments in better understanding of the problems and inventing new solutions to combat them, and therefore they are valuable assets. Although, DDoS has commercial benefits to the cyber-gangs, it has been utilized against nations. And they are akin to illegal arms trading in that they are eventually used against civilians. Therefore, cyber-terrorism and cyber-war present real threats and must be taken into serious consideration by the international community.

In conclusion, cyber-terrorism instances have clearly increased and have taken on new dimensions and models through the Internet's history. Undoubtedly, it is a real threat to many governments because it is cheaper and safer for the antagonists. Certainly, working in unison to combat it through the updating of international law, setting-up multi-national cyber-deterrence divisions, developing coherent policies and proper response strategies to cyber-terrorism and collaborations amongst governments will lead to international dispute avoidance.

Acknowledgement: Thanks to Walter Price Maguire for proof reading the article.

References: