

Abstract for submission to CCDCOE Conference on Cyber Warfare by Major J P I A G Charvat GBR A, COE DAT, Ankara, TURKEY

Terrorism and Cyberspace: the use of the Internet by terrorist organizations and the possibilities of terrorist cyber attacks.

This paper seeks to explore the possibilities that terrorists could utilise Cyberspace and engage in electronic or physical attack through IT systems. There is much debate in both Terrorism Studies and in Cyber Defence circle about the threat terrorism poses to Cyber Space and its potential as a future battlefield.

Firstly this paper will consider terrorism as an entity. There is no universally recognised definition of terrorism so the concept itself will be discussed. The criteria that differentiate terrorists from other criminals or cyber threats is in their very nature. The motivations of different terrorist groups will be considered from Single Issue terrorists, Ideological terrorists, National-Separatist terrorists and Political-Religious terrorists, the effects that the motivation will have on their modus operandi and the effects they are likely to try and achieve. This will be applied to Cyber Targeting as a method of possible attack and as a means of recruitment and propaganda.

The terrorists themselves will be discussed, the people who mastermind terrorist campaigns and the individuals who actually carry out attacks. Understanding the mindset of these people is an essential tool in any attempt to combat them.

The potential of the Internet and other cyber domains as a terrorist target will be considered. As an asymmetric threat with specific goals and aims, terrorism differs greatly from a conventional enemy. Terrorism is essentially a political activity and as such it requires a forum to give its message as wide an audience as possible. It is also a vital area to find and groom potential group members and an effective command and control tool.

Terrorism will attack its target on many levels and will seek disruption against civilian as well as government or military targets. SCADA systems provide a potential target as if infiltrated they can allow a terrorist organisation to achieve a physical effect through cyber space attack. As countries and communities become more reliant on cyber services for everyday life the potential for terrorist exploitation of this area is constantly increasing. Examples of actual events will highlight this possibility.

The paper will conclude that Cyber Terrorism is an area of extreme concern. Unlike any conventional state actor or criminal organization terrorism can seek for wanton destruction to gain attention which may be previously undetected. Terrorism is also a patient enemy and the concerns of sleeper cells within organizations make defence against cyber terrorism different to any other cyber threat.

Although ultimately the defences against cyber terrorism are physically similar to any other form of threat, there is a different mentality to consider. If this is not taken as a real and imminent possibility then the unique nature of the terrorist psyche may allow unconsidered weak points to be exploited by terrorists.

J P I A G CHARVAT
Feb 2009