August 2005

CYBERTERRORISM & CYBERCRIME

By Dr. Lionel C.M. VonFrederick Rawlins, President & CEO, The VonFrederick Group

Terror, espionage and crime are often confused when discussed in the context of Cyberspace. They are assumed to be the same when referred to as "Information Warfare." Cyberwarfare is based on such operations as viruses, Internet worms, malicious software and other forms of hacking. But Cyberterrorism and Cybercrime are very different. Cyberterrorism aims to wreak casualties and destructions through Cyberspace, allowing attackers to remain far from the target while inflicting inordinate spoliation. Such operations could reduce logistical problems of transferring explosives and other equipment. In contrast, Cybercriminals seek profit rather than spectacle. They focus on identity theft, illegal transfer of funds, money laundering, Internet fraud, tax evasion, and communications between criminal organizations.

Cyberterrorism and Cybercrime are serious ailments of the information age. In the 1980s, during the "big bang" of personal computing, it was thought that denial of hacker penetration of computers would be a manageable task. As computing and the Internet rapidly grew, the challenges of securing computer systems became increasingly perplexing and prodigal. By the mid-1990s, computer warfare – the term for attacks originating from a computer and targeting another computer or network – was regarded as the ability to exploit the extreme vulnerability of information systems. This warfare could take many forms and successes could be devastating. Espionage, terrorism, criminal intent, vandalism, anarchy or just plain youthful pranks comprise motivations for attacks on computer systems.

Realizing the severity of this threat, governments and private industries worldwide have launched intensive efforts to conceal information from the public regarding the extent of computer attacks on infrastructure and business, and industry computer systems. The reasons range from governments, intending to avoid fear and panic, to businesses (particularly financial institutions) wishing to refrain from revealing statistics on Cybertheft and fraud.

Critical systems and infrastructures are increasingly subject to Cyberattacks. Tens of millions of hacking attempts transpire annually around the world – a vast majority of them by playful teenage hackers – most of which are never detected. For instance, hundreds of thousands of attacks on U.S. Department of Defense systems are assumed to take place each year. The most optimistic estimates place the Pentagon's detection rate at five percent of all attempts (Sobelman, 2005). It is very difficult to assess how many attacks actually transpire, and worse, how many succeed without being detected. A primary danger is the relative ease with which a less-advanced opponent can inflict large-scale damage. Therefore, preventing and concealing successful attacks against computer systems are considered to be of the highest priority in most modern cities and countries. Although disclosures of attacks are rare, it is logical to assume that civilian computer systems, particularly financial institutions, are subject to significantly higher rates of penetration attempts than those of military and intelligence organizations. Rough assessments by the FBI and InterPol estimate annual losses incurred by financial institutions and high-tech industries by computer espionage, as well as other illegal financial transactions on the Internet, at hundreds of millions of dollars.

This will ultimately get worst before it gets better. It is not a quick-fix, but awareness of the severity of the problem and being dexterous, will minimize the devastation. The adoption of a Proactive Defensive Doctrine (PDD) will put in place options to protect systems and assets from intrusion and intruders. This includes intelligence gathering on terrorist and criminal groups active in Cyberspace. Academic and intelligence research should be conducted on these groups, their ideologies, aspirations and targets***. What you don't know, can hurt you.***