Is Everyone an Enemy in Cyberspace?

Ariel T. Sobelman

Introduction

Cybercrime and Cyberterror 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 difficult and costly.

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 success 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, business and industry computer systems. The reasons range from governments, intending to avoid fear and panic, and businesses (particularly financial organizations) wishing to refrain from revealing statistics on Cybertheft and fraud. The result is that the public could conclude that computer security is tolerable. In fact, this is far from being the case.

Critical systems and infrastructures are increasingly subject to Cyberattacks. Tens of millions of hacking attempts are estimated to transpire annually around the world — a vast majority of them by playful teenager 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.

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 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.

There are a number of inter-related reasons why the efforts to confront Cyberterrorism and Cybercrime have been unsuccessful. First, the two terms are often referred to as interchangeable. Another reason is that Cybercrime and Cyberterrorism are regarded as national security issues handled by defense and intelligence organizations. A third factor is that Static Defense, the strategy pursued to combat these phenomena, is purely defensive. Moreover, security agencies in various countries do not believe they can distinguish between "friend and foe." This has made them extremely reluctant to cooperate with each other in combating computer warfare. Consequently, they fail to benefit from information and experience achieved by others.

What is the difference between Cybercrime and Cyberterrorism?

Terror, espionage and crime are often confused when discussed in the context of Cyberspace. They are assumed to be the same, referred to as "Information Warfare." Cyberwarfare is based on such operations as viruses, Internet worms, malicious software and other forms of hacking. But Cybercrime and Cyberterror are very different. Cyberterrorism aims to wreak casualties and destruction through Cyberspace, allowing attackers to remain far from the target. Such operations could reduce logistical problems of transferring explosives and other equipment.

In contrast, Cybercriminals seek profit rather than spectacle. They could focus on illegal transfer of funds, money laundering, Internet fraud, tax evasion, and communications between criminal organizations.

Exclusive handling of Cyberspace threats by National Security Establishments

The similarity between various forms of Cyberattacks led national security organizations to assume responsibility. Unfortunately, the tendency to group different types of information warfare together has blocked effective measures. In most Western countries, computer warfare has been addressed by national security organizations, law enforcement authorities and the criminal justice system. But these systems have fallen short of their goals. The national security establishment has failed in stopping Cyberattacks. Law enforcement agencies lack practical tools to catch offenders and collect evidence. As a result, the criminal justice system has obtained few convictions of Cybercriminals.

The tendency to link Cyberterrorism and Cybercrime has led the U.S. national security establishment — particularly the intelligence community — to argue the same tools are needed to combat these activities. The United States, refusing to separate the various forms of computer warfare, treated every incident — including pranks by juvenile hackers — as relating to national security. This approach spread and now many other countries deal Cyberspace violations as a national security issue. Thus, it is clear why an average Israeli teenager, Ehud Tanenbaum, known as the "Analyzer" and arrested in 1998 for hacking Pentagon Web sites, was automatically suspected by U.S. authorities of being an Israeli agent.

Governments, regarding the issue as ultra-sensitive, have sought their own solutions to computer warfare, refusing to cooperate with their foreign counterparts and keeping their own programs under a blanket of secrecy.

Static Defense

Static Defense is a defensive posture adopted by most modern countries to combat computer warfare. The strategic logic behind this doctrine is that Cyberattacks are frequent, often undetectable and arrive without warning. Furthermore, the anonymity of Cyberspace and the difficulty of identifying the source of an attack make deterrence unlikely.

To make matters worse, an eerie asymmetry between technologically advanced countries and their developing counterparts has emerged. This asymmetry allows a backward country to paralyze the computer systems of a technologically-advanced enemy without being vulnerable to a similar counterattack.

Therefore, Static Defense argues that an advanced defense system is the only practical way to defend against Cyberattacks. This defense system would not rely on early warning, intelligence on impending attacks, or even awareness of an attack. Instead, Static Defense is dominated by the idea of massive single line of defense comprised of virtual fortifications and firewalls around the national information assets and computer systems. As a result, intelligence agencies would not need to spend time on monitoring hackers and their supporters or tracing their funding and technology.

"No friends — Everyone's an Enemy"

The reality of Cyberwarfare represents a departure from traditional concepts of law enforcement, terrorism and espionage. Take the issue of terrorism.

Most governments can distinguish between friend and foe and understand the connection between terrorism and organized crime. This allows for a meeting of interests and cooperation between like-minded nations. Israel and the United States, for example, share an interest in foiling sabotage plots to Israeli airliners on U.S. soil. The assumption is that Israel will do the same for the United States or any other friendly government. The possibility of espionage is always there. But experience has demonstrated that friendly governments overcome their suspicion to focus on counterterrorism cooperation and intelligence exchanges.

The same trust and spirit of cooperation is absent when it comes to Cyberspace. Instead, competition between nations regarding such information is fierce. The rules of cooperation have not yet been defined regarding computer warfare. So far, cooperation in Cyberspace seems far away. It seems that in Cyberspace there can be no friends; everyone is a potential enemy.

Summary and Recommendations

The classified nature of information technology and defense appears to preclude even the most modest dialogue between friendly nations. The inability to differentiate between national security and criminal attacks makes it extremely difficult to share defensive, technical and methodological information, because of the risk of abuse. But this attitude ignores the urgent need for international cooperation. The disadvantages of the "no friends" logic outweigh its benefits. Current levels of security remain intolerable but national solutions are inadequate. Failure to cooperate prevents solutions as well as allows Cyberattackers to remain on the loose. The only answer is a thorough review and redefinition of the policy towards Cyberwarfare.

The international community must create a mechanism for international cooperation. The elements of the cooperation should be based on the following:

1. The need to differentiate between threats: Criminal and terrorist activities in Cyberspace are not the same thing and they leave different signatures. These differences can be identified and utilized.
2. Adoption of a *proactive defensive doctrine, PPD.* This includes intelligence gathering on criminal and terrorist groups active in Cyberspace. Governments must allocate funding for intelligence gathering and research. Academic and intelligence research needs to be conducted on the groups, their ideologies, aspirations and targets.
3. Establishment of international cooperation: This includes the International Computer Emergency Response Center and CERT, law enforcement cooperation, exchange of intelligence and sharing of technical information. These activities will likely enhance trust and increase the potential for early detection and apprehension of Cyberspace abusers.

Strategic
ASSESSMENT

Strategic Assessment is a Quarterly, published by the Jaffee Center for Strategic Studies at
Tel Aviv University, Ramat Aviv, Tel Aviv 69978 Israel. Tel: (03) 640 9926 Fax: (03) 642 2404

Strategic Assessment is published in English and Hebrew.
The full text of ***Strategic Assessment*** is available on the Center's
Website: **http://www.tau.ac.il/jcss/quarterly.html**