GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

What is Cyber-terrorism?
Serge Krasavin Ph.D. MBA
July 27, 2000

In the wake of the recent computer attacks, many have been quick to jump to conclusions that a new breed of terrorism is on the rise and our country must defend itself with all possible means. As a society we have a vast operational and legal experience and proved techniques to combat terrorism, but are we ready to fight terrorism in the new arena – cyber space?

A strategic plan of a combat operation includes characterization of the enemy's goals, operational techniques, resources, and agents. Prior to taking combative actions on the legislative and operational front, one has to precisely define the enemy. That is, it is imperative to expand the definition of terrorism to include cyber-terrorism.

As a society that prides itself on impartiality of justice, we must provide clear and definitive legislative guidelines for dealing with new breed of terrorism. As things stand now, justice cannot be served as we have yet to provide a clear definition of the term. In this light, I propose to re-examine our understanding of cyber-terrorism.

There is a lot of misinterpretation in the definition cyber-terrorism, the word consisting of familiar "cyber" and less familiar "terrorism". While "cyber" is anything related to our tool of trade, terrorism by nature is difficult to define. Even the U.S. government cannot agree on one single definition. The old maxim, "One man's terrorist is another man's freedom fighter" is still alive and well.

The ambiguity in the definition brings indistinctness in action, as D. Denning pointed in her work Activism, Hactivism and Cyberterrorism, "an e-mail bomb may be considered hacktivism by some and cyber-terrorism by others"

It follows that there is a degree of "understanding" of the meanings of cyber-terrorism, either from the popular media, other secondary sources, or personal experience; however, the specialists' use different definitions of the meaning. Cyber-terrorism as well as other contemporary "terrorisms" (bioterrorism, chemical terrorism, etc.) appeared as a mixture of words terrorism and a meaning of an area of application. Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, who in 1997 was attributed for creation of the term "Cyberterrorism", defined cyber-terrorism as the convergence of cybernetics and terrorism. In the same year Mark Pollitt, special agent for the FBI, offers a working definition: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents."

Since that time the word cyber-terrorism has entered into the lexicon of IT security specialists and terrorist experts and the word list of mass media "professionals". One of the experts, a police chief, offers his version of definition: "Cyber-terrorism – attacking sabotage-prone targets by computer – poses potentially disastrous consequences for our incredibly computer-dependent society."

The media often use cyber-terrorism term quite deliberately: "Canadian boy admits cyberterrorism of his family: "Emeryville, Ontario (Reuter) - A 15-year-old Canadian boy has admitted he was responsible for months of notorious high-tech pranks that terrorized his own family, police said Monday"

A renowned expert Dorothy Denning defined cyber-terrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives". R. Stark from the SMS University defines cyber-terrorism as " any attack against an information function, regardless of the means"

Under the above-mentioned definitions of cyber-terrorism one can only point to the fact that any telecommunications infrastructure attack, including site defacing and other computer pranks, constitute terrorism. It means that cyber-terrorism has already occurred and we "live " in the epoch of cyber terror.

However, another expert, James Christy the law enforcement and counterintelligence coordinator for the DIAP (Defense-wide Information Assurance Program), which is steered by the office of the assistant secretary of defense for command, control, communications and intelligence, states that cyber-terrorism has never been waged against the United States. "Rather, recent hacking events – including a 1998 web page set up by a

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

supporter of the Mexican Zapatistas rebel group, which led to attacks on the U.S. military from 1,500 locations in 50 different countries – constitute computer crime. William Church, a former U.S. Army Intelligence officer, who founded the Center for Infrastructural Warfare Studies (CIWARS) agrees that the United States has not seen a cyber terrorist threat from terrorists using information warfare techniques. "None of the groups that are conventionally defined as terrorist groups have used information weapons against the infrastructure" Richard Clarke, national co-ordinator for security, infrastructure protection and counterterrorism at the National Security Council offered to stop using "cyberterrorism" and use "information warfare " instead

The above-mentioned observations drive a clear line between cyber-terrorism and cyber crime and allow us to define cyber-terrorism as: **Use of information technology and means by terrorist groups and agents.**

In defining the cyber terrorist activity it is necessary to segment of action and motivation. There is no doubt that acts of hacking can have the same consequences as acts of terrorism but in the legal sense the intentional abuse of the information cyberspace must be a part of the terrorist campaign or an action.

Examples of cyber terrorist activity may include use of information technology to organize and carry out attacks, support groups activities and perception-management campaigns. Experts agree that many terrorist groups such as Osama bin Ladenn organization and the Islamic militant group Hamas have adopted new information technology as a means to conduct operations without being detected by counter terrorist officials.

Thus, use of information technology and means by terrorist groups and agents constitute cyber-terrorism. Other activities, so richly glamorized by the media, should be defined as cyber crime.

List of References:

Ch. Arthur and N. von Herberstein. "Cyberterror attack rocks America" Independent 05/03/98 p 1. http://www.info-sec.com/denial/denial_030498a.html-ssi (07.20.00)

Find Law website. http://www.findlaw.com/scripts/search.pl?CiRestriction=cyberterrorism Find Law website site and its legal dictionaries produce "No matches" on cyberterrorism (07.20.00)

The Terrorism research center http://www.terrorism.com/. FBI definition: "Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives". Department of State definition: "The term 'terrorism' means premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents." (07.20.00)

Dorothy E. Denning. " Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" http://www.nautilus.org/info-policy/workshop/papers/denning.html (06.07.00)

Barry Collin. "The Future of CyberTerrorism", Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, 1996

Mark M. Pollitt. "A Cyberterrorism Fact or Fancy?", Proceedings of the 20th National Information Systems Security Conference, 1997, pp. 285-289

William H. Webster and Arnaud de Borchgrave. "Cybercrime, Cyberterrorism, Cyberwarfare". The Center for Strategic and International Studies Global Organized Crime Project. http://www.csis.org/pubs/cyberfor.html (06.15.00)

Dave Pettinari "**Cyber terrorism, information warfare, and attacks being launched now and in the future in the heartland of America", Police Futurists International.** http://www.policefuturists.org/fall97/terror.html (06.20.00)

REUTER. "Canadian boy admits cyber terrorism of his family" http://www.infowar.com/class_1/Class1_y7.html-ssi (06.20.00)

Dorothy E. Denning. "CYBERTERRORISM" Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Georgetown University May 23, 2000

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (06.20.00)

Rod Stark. "Cyber Terrorism: Rethinking New Technology". Department of Defense & Strategic Studies Graduate Assistant Southwest Missouri State University http://www.infowar.com/mil_c4i/stark/Cyber_Terrorism-Rethinking_New_Technology1.html (06.06.15)

Catherine MacRae. "Cybercrime Vs Cyber Terrorism, DOD Official Says U.S. Has Been Victim Of Cyber Crimes, Not Terrorism". Defense Information and Electronics Report, 10/01/99

John Borland. "Analyzing The Threat Of Cyberterrorism". TechWeb News. http://www.techweb.com/wire/story/TWB19980923S0016 (07.20.00)

Dan Verton "Are cyberterrorists for real?" Federal Computer Week. 06.26.2000 http://www.fcw.com/fcw/articles/2000/0626/pol-terror-06-26-00.asp (07.20.00)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.