Drexel UNIVERSITY

CYBER TERRORISM: HACKERS BECOMING TERRORISTS OR TERRORISTS BECOMING HACKERS?

ABSTRACT

(key arguments)

LACK OF CYBER SKILLS IS AN OBSTACLE FOR TERRORISTS BUT IT CAN BE ADDRESSED BY TRAINING / HIRING / RECRUITING ROGERS' (1999) HACKER TAXONOMY IS USED TO IDENTIFY CRIMINAL HACKERS, FOLLOWED BY PROFILE MATCH OF HACKERS AND TERRORISTS * WE TRY TO IDENTIFY A DEFINITION OF CYBER-TERRORISM THAT WOULD ENABLE US TO IDENTIFY TRUE CYBER-THREATS.

DEFINING CYBER-TERRORISM (CT)

CT → CYBER + TERRORISM

REFERS TO:

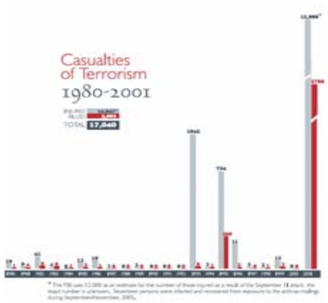
* MODE OF ATTACK
* VENUE OR TARGET

E.g. Information systems

TERRORISM ACCORDING TO STOHL (1988):

PURPOSEFUL ACT OR THREAT OF ACT OF **VIOLENCE** TO CREATE FEAR AND/OR COMPLIANT BEHAVIOR IN VICTIM AND /OR AUDIENCE OF THE ACT OR THREAT.

MYTH: TERRORISM SYNONYMOUS WITH DEATH AND DESTRUCTION.



Source: Terrorism 2000/2001, Federal bureau of investigations (FBI)

TOTAL CASUALITIES (1981-2001) AS A RESULT OF TERRORISM= 2,993

TOTAL FATALITIES IN 2003 ALONE, ACCORDING TO F.A.R.S.= 38,252
http://www-fars.nhtsa.dot.gov

Highway deaths (2003) ~ 10 * casualties as result of terrorist (1981-2001)

ROGERS' (1999) HACKER TAXONOMY

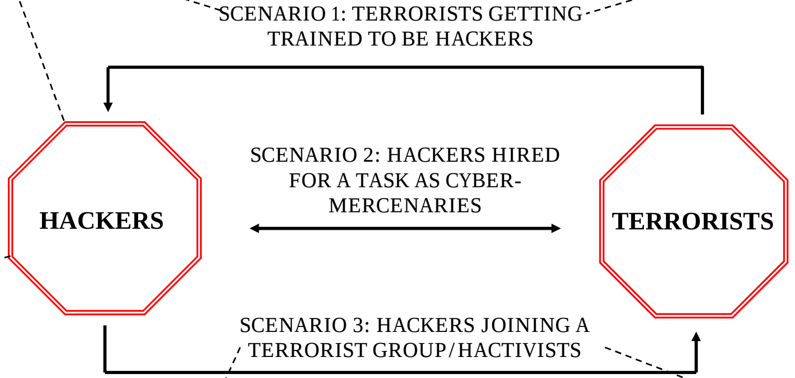
- OLD SCHOOL HACKERS/ OLD GUARDS
- NEWBIE/TOOLKIT & CYBER-PUNKS
- VIRUS / CODE WRITERS & INTERNALS
- PROFESSIONAL CYBERCRIMINALS / CRACKERS

(COLOR INDICATES THE THREAT LEVEL POSED BY EACH CATEGORY)

CYBER TERROR CAPABILITY (Source: Center for study of terrorism and irregular warfare)	
Level I, Simple-unstructured	Old School hackers, Script Kiddies/Cyber Punks, Professional Criminals, Virus Writers
Level II, Advanced-Structured	Old School hackers, Professional Criminals/ Crackers, Virus Writers/Code breakers
Level III, Complex-coordinated	Old School Hackers and Professional Crackers

POSSIBLE TRAINING RESOURCES: ETHICAL HACKING CERTIFICATION

* **Topics taught:** General security, counter hacking, Wireless security,intrusion detection
* **Pre-requisites:** Working knowledge of OS, TCP/IP, some network tools exposure
* **Concerns**:Lack of background checks for candidates, sometimes a legal agreement signed that new found skills would not be misused.


SCENARIO 1: TERRORISTS GETTING TRAINED TO BE HACKERS
HACKERS
SCENARIO 2: HACKERS HIRED FOR A TASK AS CYBER-MERCENARIES
TERRORISTS
SCENARIO 3: HACKERS JOINING A TERRORIST GROUP/HACTIVISTS

PROFILE MATCH based on:

*AGE, SEX, MARITAL STATUS, ECONOMIC STATUS, EDUCATION, CRIMINAL RECORD

* COMPARING OF MOTIVATIONS OF HACKERS AND TERRORISTS

* COMPARISON BETWEEN THE PATHWAYS TO BECOME A HACKER, AND PATHWAYS TO BECOME A TERRORIST

* PSYCHOLOGICAL AND SOCIOLOGICAL THEORIES FOR CRIMINAL BEHAVIOR

KNOWN THREATS

1. SCADA: Supervisory Control and Data Acquisition

• Built on the assumption that these systems would b "**AIR GAPPED**" or disconnected form external network. Systems already in place for controlling power grids etc., they have **too many security hol** to plug. **Retro-active security measures** taken or systems demanding high-security will always have loop-holes.

2. SOCIAL ENGINEERING

• Cyber-attacks initiated from within an organization **Lack of responsible security behavior**, facilitate security break-ins.

3. WMD: Weapons of Mass Disruption

POSSIBLE THREATS

• **Distributed and numerous small attacks**, targeted at destroying **INTERNET TRUST in online services**. Limited cyber-skills required for this purpose.

• **Recruitment efforts and Propaganda distributio** targeted at average computer users. **Financing** for terrorists.

SELECTED REFERENCE(S):

1) Blackburn, R. (1993) The psychology of criminal conduct: Theory, research and practice. *Toronto: John Wiley & Sons*

2) Denning, D. (2001), Cyberwarriors: Activists and terrorists turn to cyberspace. *Harvard International Review, 23*(2) 70.

3) Flemming, P. and Stohl, M. (2000). Myths and realities of cyberterrorism. In *Proceedings of the International Conference on Countering Terrorism through Enhanced International Cooperation*

4) Hudson, Rex A. (1999). The sociology and psychology of terrorism Who becomes a terrorist and why? *Federal Research Division, Librar of Congress*, LC Control Number: 2003426357.

5) Post, J. (1996). The dangerous information system insider: Psychological perspectives. *Available HTTP: Hostname: infowar.con*

6) Rogers, M. (1999) "Psychology of Hackers: Steps Toward a New Taxonomy" *Hacker Sitings and News* *http://www.infowar.com/hacker/99/HackerTaxonomy.shtml* 25/7

CONTACT AUTHOR(S):

GEORGE ABRAHAM
(SGA72@DREXEL.EDU)

LEW HASSELL, Ph.D.
(LEW.HASSELL@CIS.DREXEL.EDU)

REFERENCES (JOURNALS):

1) Blackburn, R. (1993) The psychology of criminal conduct: Theory, research and practice. *Toronto: John Wiley & Sons*

2) Denning, D. (2001), Cyberwarriors: Activists and terrorists turn to cyberspace. *Harvard International Review, 23*(2) 70.

3) Flemming, P. and Stohl, M. (2000). Myths and realities of cyberterrorism. In *Proceedings of the International Conference on Countering Terrorism through Enhanced International Cooperation*

4) Hudson, Rex A. (1999). The sociology and psychology of terrorism: Who becomes a terrorist and why? *Federal Research Division, Library of Congress,* LC Control Number: 2003426357.

5) Post, J. (1996). The dangerous information system insider: Psychological perspectives. *Available HTTP: Hostname: infowar.com*

6) Rogers, M. (1999) "Psychology of Hackers: Steps Toward a New Taxonomy" *Hacker Sitings and News* *http://www.infowar.com/hacker/99/HackerTaxonomy.shtml* 25/7/01.

REFERENCES (Websites):

1) http://faculty.ncwc.edu/toconnor/429/429lect02.htm
http://faculty.ncwc.edu/toconnor/429/429lect01.htm
Provide a snap shot view on all the theories in terrorism and very good read overall to get an idea about what scholars and the literature have to say about terrorism.

2) http://www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html
The author talks about the vulnerability of SCADA networks and the inherent design flaws in security for this system which controls power grids etc.

3) http://edition.cnn.com/TECH/specials/hackers/cyberterror/
CNN report on cyberterror.

4) http://ref.web.cern.ch/ref/CERN/CNL/2000/003/scada/
Definition of SCADA, a review of the software architecture. Information of the inner workings of the system with schematics.

5) http://www.edu.uni-klu.ac.at/~epirker/unix/hacker-howto.html
Gives pointers as to what has to be done to be known as a hacker. The author is a hacker himself and talks about the hacker motivations, attitude etc. In other words and insider view of hacking. He clearly differentiates and validates Rogers findings regarding crackers and hackers being two distinct groups. Another comprehensive source is: http://www.catb.org/~esr/faqs/hacker-howto.html

6) http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=109
Anthony Stahelski has argued for the fact that Terrorists Are Made, Not Born: Creating Terrorists Using Social Psychological Conditioning. He has put forth the five phases of Psychological conditioning.