



# Cyber Forensics' Role in the War on Terrorism

2006 Expert Public Safety  
Symposium  
Copenhagen, Denmark  
October 11, 2006



Marcus Rogers PhD, CISSP,  
Associate Professor  
Purdue University  
Kathryn Scarborough, PhD  
Professor  
Eastern Kentucky University

© 2006 Purdue University & Eastern Kentucky  
University



## Outline

- Post 9/11
- The Changing U.S. State and Local Law Enforcement Role
- Terrorists & Technology
- It's More than Cyber Terrorism
- Intelligence
- Cyber Forensics & Intel
- Issues
- Efforts
- Summary

© 2006 Purdue University & Eastern Kentucky University



## Post 9/11

- Terrorism is not new
- What is new are the techniques, not necessarily the ideology
- Our response to terrorism and our counter terrorism efforts need to evolve
- Intelligence is one of the most vital weapons in our arsenal and needs to be used more effectively

© 2006 Purdue University & Eastern Kentucky University

## The Changing State of U.S. Local Law Enforcement Role

- Terrorism is no longer just a Federal responsibility!
- State and Local Law Enforcement (SLE) must be involved
  - Formally through Federal Bureau of Investigation's Joint Terrorism Task Forces
  - Informally through intelligence sharing
- SLE's are now seen as the "front line" in the U.S. for counter terrorism
  - 17,784 State and local law enforcement agencies (SLE)
  - 796,518 officers nationwide

© 2006 Purdue University & Eastern Kentucky University

## Terrorists & Technology

- Technological advances have not been ignored by terrorists
- Technology has become an enabler for the "business" of terrorism
- Technology is used by terrorists for:
  - Communications
  - Marketing & Propaganda
  - Recruiting
  - Fund Raising
  - Intelligence gathering, development, and sharing
  - A weapon
  - A target

© 2006 Purdue University & Eastern Kentucky University



## It's More than Cyber Terrorism

- Focus has previously been on technology as a target
  - This is too limited!
- Critical Infrastructure Protection
  - The Internet is the backbone
- What about the other uses of technology?

© 2006 Purdue University & Eastern Kentucky University



## Intelligence

- The 9/11 Commission indicated that intelligence is a key in the current counter terrorism effort
- SLE's have been criticized for a lack of intel capabilities; federal agencies have been criticized for their limited assistance
- DHS has been criticized for overlooking or underestimating the importance of SLE's and limiting their attention to intelligence and cyber security

© 2006 Purdue University & Eastern Kentucky University

# Cyber Forensics & Intelligence

- Technology is a primary tool for developing and sharing intel
  - Wiretaps
  - Datataps
  - Netflow analyses
  - Storage analyses
  - Data Mining
- Cyber Forensics is an information gathering tool!
  - It's all about the "bits"

© 2006 Purdue University & Eastern Kentucky University

# Cyber Forensics & Intelligence

## Cyber Forensics

Identification  
Collection  
Examination  
Analysis  
Report

## Intelligence Analysis

Identification  
Collection  
Processing/Development  
Analysis/Interpretation  
Dissemination

© 2006 Purdue University & Eastern Kentucky University



## Cyber Forensics & Intel

- Current Issues
  - Lack of communications and information sharing
  - Lack of training related to digital evidence and technology in general
  - Forensic tools as intel analysis tools
  - Lack of IT networking knowledge
  - Real lack of training related to intel gathering during the forensic/investigative process
  - Forensics and Intelligence are related but not identical
  - When does the need for intel trump the need to convict?

© 2006 Purdue University & Eastern Kentucky University



## Efforts

- Purdue & NW3C
  - DHS Competitive Training grant
- Objective/Goals
  - Provide a comprehensive computer crime training curriculum that specializes in the identification of "terrorist acts via computer aided devices" in order to enhance nationwide State and local law enforcement agencies ability to assist Federal agencies in the prevention, identification, and prosecution of Acts of Terrorism.

© 2006 Purdue University & Eastern Kentucky University



## Efforts

- Develop and deliver courses related to:
  - Advanced criminal intelligence training to prevent terrorism
  - Fast Forensic Triage
  - Information Security for SLE
- Pilot Phase will train 750 SLE Officers

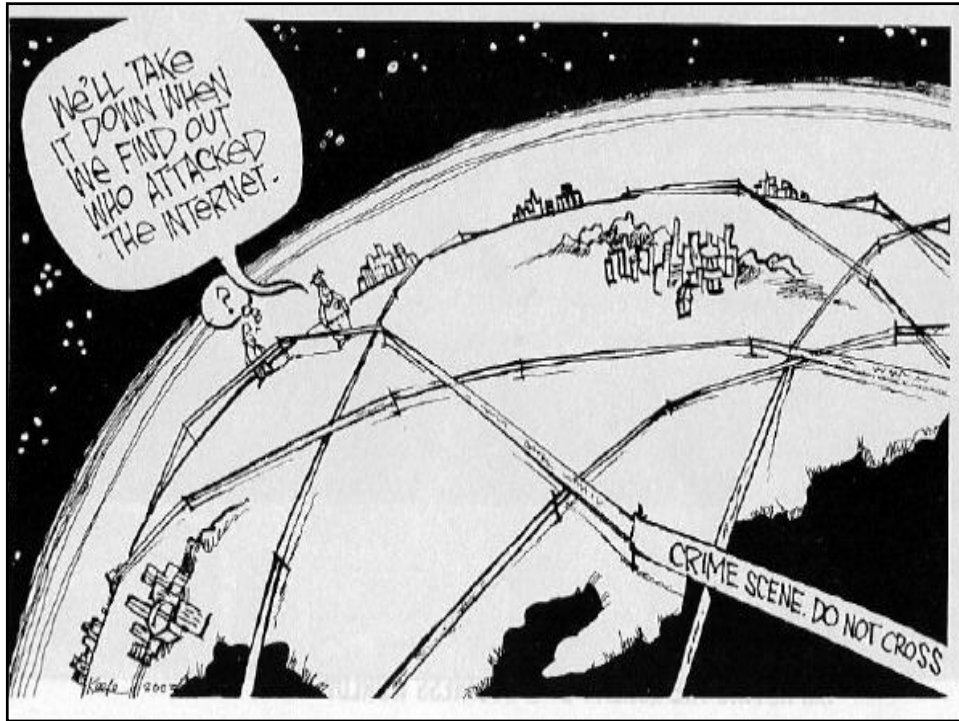
© 2006 Purdue University & Eastern Kentucky University



## Summary

- Terrorism is not going away any time soon
- Terrorist organizations use and/or target technology
- SLE are really the front line in U.S. domestic counter terrorism
- The role of intelligence cannot be underestimated
- Technology is a fertile source of intelligence
- Cyber forensics is an effective but overlooked information gathering & analysis tool
- Proper training is needed
- Better communications is required
- Cyber forensics can be used as an early warning system
- Efforts are under way, but much more work is needed

© 2006 Purdue University & Eastern Kentucky University





## Contact Information

Dr. Marcus Rogers  
rogersmk@purdue.edu

<http://www.cyberforensics.purdue.edu>

Dr. Kathryn Scarborough  
kscarbocop@aol.com

© 2006 Purdue University & Eastern Kentucky  
University