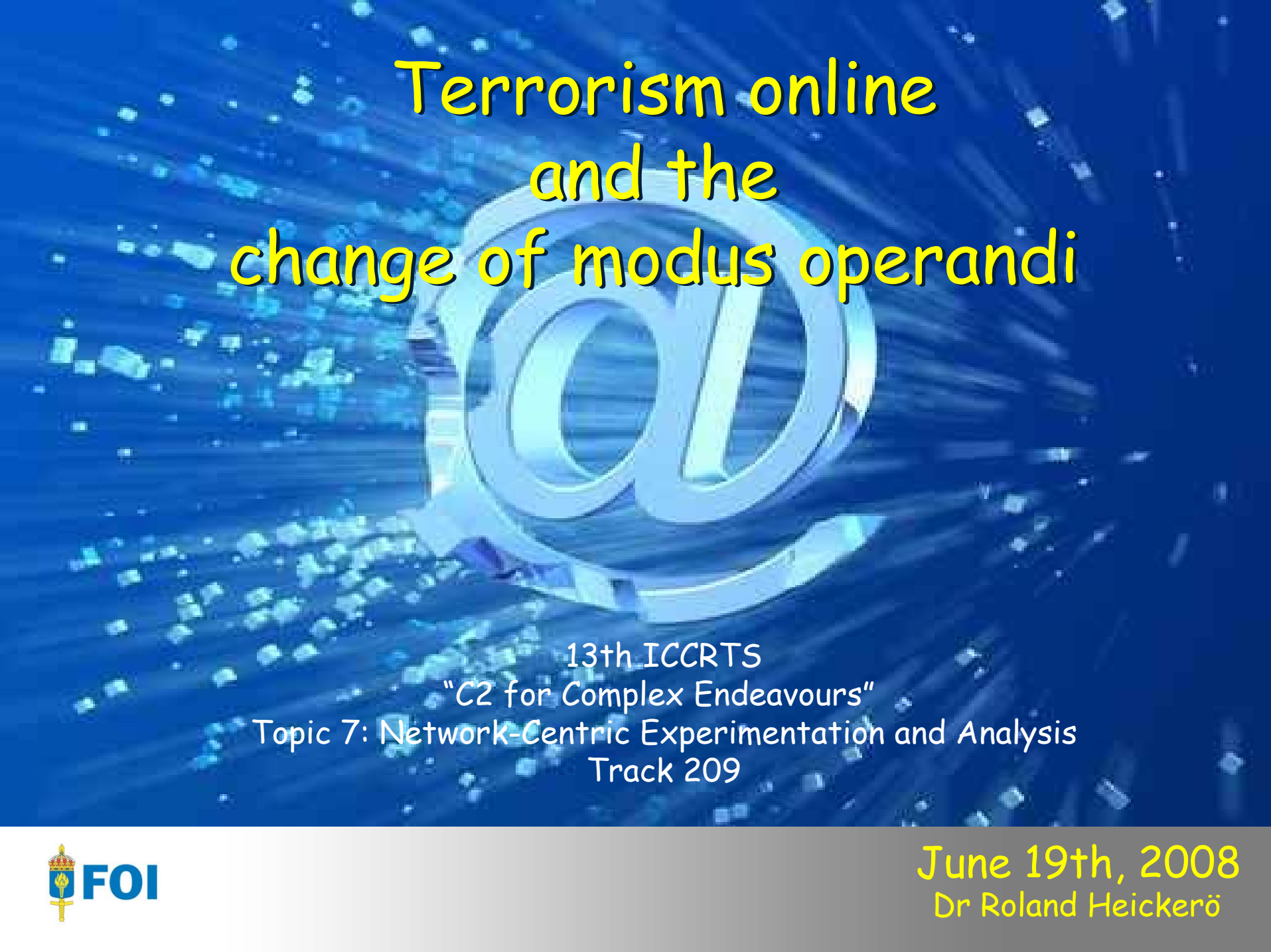
Terrorism online and the change of modus operandi



13th ICCRTS
"C2 for Complex Endeavours"
Topic 7: Network-Centric Experimentation and Analysis
Track 209

FOI

June 19th, 2008

Dr Roland Heickerö

Purpose

The purpose is to describe the development of new types of electronic and digital threats on the society such as cyber terrorism

Insurgent's motives, logic and usage of information warfare means and weapons are discussed

FOI

Outline

- Principles of information warfare
- Effects of cyber attacks
- Differences between "traditional" terrorism & cyber terrorism
- Actors and antagonists within cyber space
- Change of cyber terrorism modus operandi; the al-Qaeda example
- Conclusions

FOI

Principles of Information Warfare

FOI

Assumptions

The modern society is getting more and more dependent on electronics, advanced telecommunications, energy supply systems, information/computer networks etc. A cyber attack against these systems will lead to serious consequences for the society, for companies as well as individuals

The systems have *inherent* a number of vulnerabilities and dependencies. For instance, if the power resources are crippled it cause a cascading outage that can cripple the complete ICT system

FOI

Information warfare comprise of:

… against networks, information and communication systems as well as the produced information

FOI

Information Warfare

- With Computer Network Operation (CNO) & Electronic Warfare (EW) weapons it is possible to attack critical infrastructure
- Asymmetrical approach; cheap, cost effective
- Act anonymously – difficult to identify the aggressor
- Long distance
- Tools for CNO could be used for protection as well as attacks
- No rules in digital world, legal implications

FOI

Effects of cyber attacks

Physical effects: physical destruction of information structures with the consequences that the information system could not be used properly (DOS), to knock out electronics with EW weapons such as EMP

Syntax effects: to attack system logic by delaying information and to develop unpredictable behaviors using CNO tools (viruses, trojans, hacking)

Semantic effects: to destroy the trust in a system by manipulation, change of information and deception that affect the decision making process

FOI

"Traditional" terrorism & cyber terrorism

Terrorism in general

Definition: "…violence or threat of violence, used and directed in pursuit of, or in service of political aim" (Hoffman, 1998)

Classification:

a) political-ideological
b) ethnical-religious
c) state sponsored
d) criminal driven

"Traditional" terrorism

Logic: Terrorism is based on fear, unpredictable attacks, chock effects, grandiose, asymmetric, mass media attention

Means & methods: Suicide bombers, explosives, strive to get weapons for mass destruction, the Internet could be used as a tool for coordination of activities

FOI

Cyber terrorism

Cyber: terrorism Generic term for a number of hostile activities against critical information infrastructure such as the SCADA system, fear for an "electronic Pearl Harbor"

Logic: Well educated individuals, good knowledge of IT-systems, no suicide bombers but with a political-religious cause, media attention is not necessary a goal

Two: opinions a) The threat is massive or b) exaggerated, no casualties so far…

FOI

Actors and antagonists in the cyber space

Types:

a) script kiddies
b) crackers, hackers and hacktivists
c) cyber terrorists
d) insiders

Organizations:

Hierarchical, decentralized, ad-hoc networks autonomous cells etc.

Resources:

Personal, economical and logistical, knowledge in and access to CNO and EW weapons

FOI

Resources and means

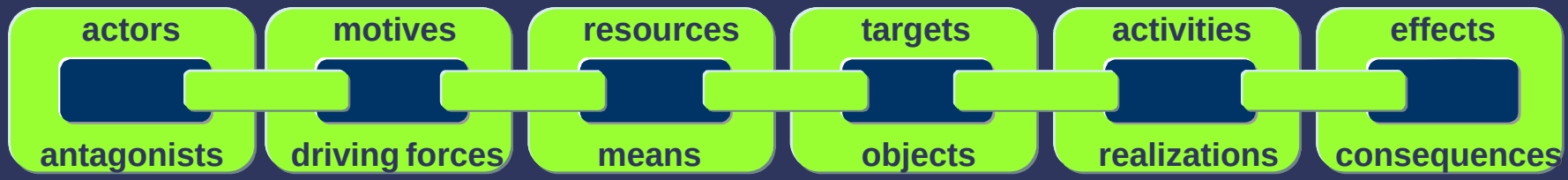
Cyber weapons: logical bombs, worms, viruses, and trojans, EW equipment for monitoring and jamming, EMP pulse weapon, BOT nets used for DOS-attacks

Actions: remote, long distance, closed peer-to-peer networks, avoid digital tracking, stegonography, use the Internet for co-ordination, information seeking, social engineering

Targets: depends on the objectives and available means and resources, mainly civilian

FOI

Actor-target-effect chain



(organizational structures, risk willingness, ethical/moral limitations)

(social, psychological, economical, political)

(weapons, economy, methods, logistics, personal)

(infrastructure, organizations, individuals, symbols)

(planning, realization, disorganization, revision)

(physical. syntax, semantic effects immediate-indirect)

FOI

Information available on the Internet

… the locations of target objects…

FOI

Information available on the Internet

…blueprints describing the target

FOI

Information available on the Internet

…equipment to be used…

EMP Shock Generators

Information available on the Internet

… how to purchase and the costs …

Assembled shock wave generators in choice of 28 vdc or 115 vac
Pulse rate 20 per minute - Require emitter antenna.

EMP150 - 150 Joules 15 KV 20 KA.....**$3495.00**
EMP250 - 250 Joules 25 KV 30 KA.....**$4795.00**
EMP400 - 400 Joules 40 KV 45 KA.....**$6495.00**

… to be ordered at www…

FOI

Information available on the Internet

… and bulletin boards discussing security holes, vulnerabilities within computer systems, how to download and use malware, methods on how to conduct hacker activities …etc.

FOI

Change of cyber terrorism modus operandi; the al-Qaeda example

FOI

The terror organization enters the cyber arena

"In matter of time, you will se attacks on the stock market. I would not be surprised if tomorrow, I hear of a big economic collapse because of somebody attacking the main technical systems in big companies"

e-mail correspondence in 2005 between al-Muajirun leader Omar Bakri to a well known al-Qaeda sympathizer

"…that hundreds of young men have pledged to him that they were ready to die and that hundreds of Muslims scientist were with him and who would use their knowledge in chemistry, biology and ranging from computer to electronics against infidels"

Bin Ladin to Hamid Mir, editor of newspaper Ausuf

FOI

Strategy and way of working

… using dispatchers for co-ordinate information gathering about target objects, to synchronize contact people towards hackers & cracker community,

… method based on piece of a puzzle

FOI

al – Qaeda top management

Example of possible process in order to prepare for a cyber operation

Dispatchers

Unix

Networks

Windows

Data bases

Contact persons

Bulletin boards, hacker community

@ @ @ @ @ @

FOI

al – Qaeda top management

Information about target object is requested

Questions on vulnerabilities and methods how to attack

Dispatchers

Unix | Networks | Windows | Data bases

Sub questions added to contact persons

Contact persons

Fake usernames, add questions

Bulletin boards, hacker community

@ @ @ @ @ @

FOI

al – Qaeda top management

Order a cyber attack!

Analysis, suggestion on methods how to attack target object

Dispatchers

Unix | Networks | Windows | Data bases

Picture of target system and its vulnerabilities

Contact persons

Answers from the boards

Bulletin boards, hacker community

@ @ @ @ @ @

Why using dispatchers?

+ Reduce the own network vulnerabilities
+ Limit the cyber terror network knowledge of its own size and channels
+ Reduce damage if counter insurgency authorities discover the network

FOI

Conclusions

-Terrorism in the cyber arena is a growing problem

- In order to reduce danger to the open society from online threats it is important to gain knowledge and to develop strategies for counter actions

- The methods has to be adapted to the change of insurgent logic and modus operandi

- Co-operation between law enforcement agencies and organizations around the globe is a necessity

FOI

FOI

roland.heickero@foi.se

Some pictures are provided by fotolia