

## CYBER TERRORISM

### How Terrorists use the Internet

10th August 2007, Chaos Communication Camp

Dr. Marco Gercke  
Lecturer at the University of Cologne, Germany  
Expert for the Council of Europe

## TERRORISM

### DECREE-LAW No. 144 (Italy)

- Since the 2001 attacks in New York terrorism is intensively used as justification for stricter laws (“anti-terrorism legislation”)
- Terrorism is a term that is used to describe a phenomenon
- It is not a justification or explanation for the need to implement stricter laws.

Obligation to request an authorisation prior to making Internet services available for the public (Internet cafe).

Obligation to install an identification procedure prior to the use of public communication services.

## DEFINITION

- Various approaches to define terrorism
- Great differences in the national definitions until now

## EU FRAMEWORKD. TERRORISM

### Terrorist offences

- aim to seriously destabilise or destroy the fundamental political structure of a country
- by attacks upon a person's life

## CYBER TERRORISM

- Very few reports published about successful Internet attacks from subversive groups
- Successful attacks are treated like state secrets to prevent chaos as well as the publication of weaknesses

## 2005 FBI ASS. DIRECTOR LOUIS REIGEL

In December 2005 the Associated Press cites US FBI assistant director as stating that Al Qaeda and related terrorist networks are presently incapable of mounting cyber-attacks that could damage US critical infrastructure.

## CYBER TERRORISM

### CRITICAL INFRASTRUCTURE

Picture removed in print version

- Discussion about cyber terrorism was for a long time concentrating on attacks against critical infrastructure
- Reason: Vulnerability of information technology
- Possible Targets: Electricity Supply, Traffic Control, Economy in general

## CYBER TERRORISM

### AL QAEDA TRAINING MANUAL

#### Main activities:

- Research
- Publishing Information (recruitment)
- Communication between members of terrorist groups
- Terrorist financing and money laundering
- Committing Cybercrime (political motivated attacks)

“Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of all information required about the enemy”

## ORGANISATION

- Decentralised structure of subversive organisations is supported by decentralised structure of the Internet
- Lack of physical territory and infrastructure is compensated by network infrastructure (virtual territory)
- Redundancy of the networks ensures the operability even if cells are uncovered
- Flexibility of modern communication allows quick reconstruction of destroyed structures (Afghanistan)
- International dimension of the Internet allow the terrorists to play an international role

## COLLECTING INFORMATION

### MILITARY INFRASTRUCTURE

- Internet is used as an information media by the subversive groups as well as by regular users
- Search-engines and data-mining strategies are supporting terrorists in gathering information about possible targets and security measures
- Additional Services (eg. Google Maps) can support the planning of attacks

Picture removed in print version

## COLLECTING INFORMATION

Telegraph.co.uk (13.01.2007)

- Services like Google Earth were reported to be used in several attacks - among them attacks against British troops in Afghanistan and the planned attacks against an airport in the US

Terrorists attacking British bases in Basra are using aerial footage displayed by the Google Earth internet tool to pinpoint their attacks, say Army intelligence sources. Documents seized during raids on the homes of insurgents last week uncovered print-outs from photographs taken from Google. The satellite photographs show in detail the buildings inside the bases and vulnerable areas such as tented accommodation, lavatory blocks and where lightly armoured Land Rovers are parked. Written on the back of one set of photographs taken of the Shatt al Arab Hotel, headquarters for the 1,000 men of the Staffordshire Regiment battle group, officers found the camp's precise longitude and latitude. "This is evidence as far as we are concerned for planning terrorist attacks," said an intelligence officer with the Royal Green Jackets battle group. "Who would otherwise have Google Earth imagery of one of our bases?"

## COLLECTING INFORMATION

TERRORIST HANDBOOK

- In the past secret information were accidentally published on websites
- Robots used by search-engines can lead the disclose of secret information
- Handbooks on how to build explosives and construct chemical and even nuclear devices are available
- Internet sources have been reported to be used by the offenders in a number of recent attacks

Picture removed in print version

## USE AS FORUM

## TERRORIST WEBSITE

- In 1998 only 12 out of 30 terrorist groups that were listed by the US State Department had Internet websites
- By 2004 nearly all terrorist groups – among them Hamas and the Hisbollah – used websites to publish information about their organisation

Picture removed in print version

## USE AS FORUM

## TERRORIST WEBSITE

### Advantages

- Possibility of anonymous set-up of a webpage (free Webspaces)
- Potential number of Users
- Worldwide access
- Low costs for the production compared to press media
- Interest of the media to use the internet as source for news coverage

Picture removed in print version

## USE AS FORUM

### TERRORIST WEBSITE

#### Content

Picture removed in print version

- Information (targeting donators)
- Means of image building (videotaped execution of foreigners)
- Disinformation

## RECRUITMENT

- Internet offers the possibility of global recruitment
- Data of users accessing information webpages of subversive groups are used by those groups to individually contact those users afterwards
- Possibilities of interactive online interaction (Chat, Voice over IP) increased to possibilities of recruitment

## USE FOR COMMUNICATION

### PUBLIC TERMINAL

Picture removed in print version

#### Advantages:

- Easy access (Internet Cafes, Wireless LAN, Mobile Internet Services)
- Very little regulation (about not restriction with regard to the anonymous use of internet services in public internet cafes)
- Very little control of law enforcement authorities
- Means of anonymous communication
- Speed of the information exchange

## USE FOR COMMUNICATION

### RESISTANCE AGAINST ATTACKS

- Use of encryption technology and means of anonymous communication can seriously hinder investigations
- The law enforcement agencies in majority of countries are not prepared for this challenge
- Background for the current debate about new investigation instruments

There is a physical argument that a 128 bit key is secure against brute force attack. It is argued that, by the laws of physics, in order to simply flip through the possible values for a 128-bit key one would need a device consuming at a minimum 10 gigawatts (about the equivalent of eight large, dedicated nuclear reactors) running continuously for 100 years.



## TERRORIST FINANCING

### ME FINANCIAL ACTION TASK FORCE

- Most terrorist networks depend up to a large degree on donations
- Internet supports the global fundraising
- Information about accounts that can be used for donations are published throughout the internet
- Specialised software tools and SPAM-Databases are used to identify potential supporters that should be contacted individually
- Virtual currencies (e-gold) and online payment services (PayPal) can be used to hide the identity of the donators

Bahrain, Saudi Arabia, Syria, Lebanon, Qatar, Kuwait, Tunisia, Jordan, Algeria, Morocco, Egypt, Oman, the United Arab Emirates and Yemen

## TERRORIST FINANCING

- Terrorist financing = reverse money laundering
- Money laundering: ML is concerned with laundering assets of illegal origin and bringing them back into legal economic circulation
- Terrorist financing: TF is concerned with using legal assets for an illegal activity
- Where did the money come from (ML) / Where did the money go (TF)
- Means and methods to identify ML can not be transferred to TF detection
- In addition there is a lack of international objective definition of the criteria of a terrorist

## HOW IT WORKS

- Regular (fake) business is set up by supporters of subversive groups
- Shop offers goods for high prices
- Donation buy an overpriced product to indirectly donate

## CONCLUSION

- Terrorists use the Internet
- The extend and intensity is (until now) staying below classic Cybercrime
- Questionable if it is necessary to address the problem with new provisions

## CONTACT

THANK YOU FOR YOUR ATTENTION



Dr. Marco Gercke  
[www.cybercrime.de](http://www.cybercrime.de)