

# CHALLENGE OF DRAFTING CYBERCRIME LEGISLATION

WSIS FORUM 2010

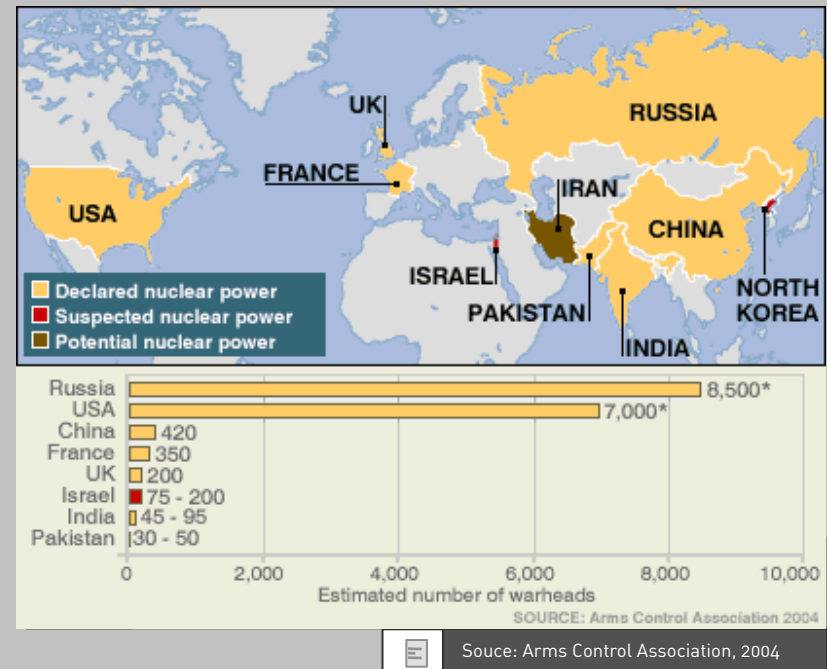
13.05.2010

Dr. Marco Gercke, Director Cybercrime Research Institute

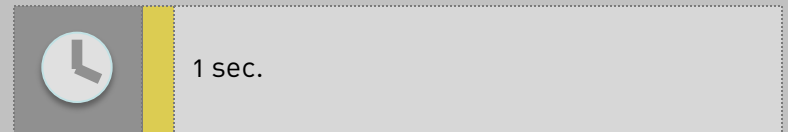
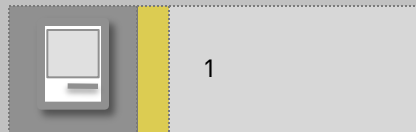
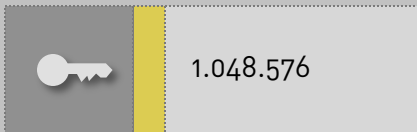
REAL WORLD = CYBER

## POWER

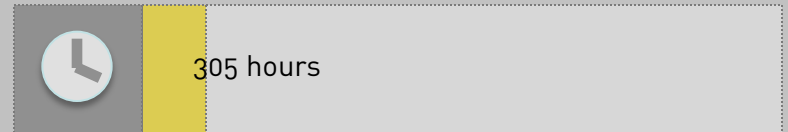
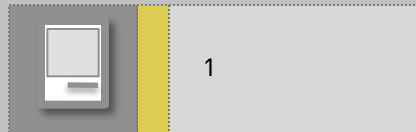
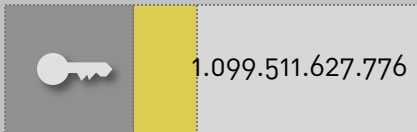
- Without doubt NATO is in military terms a powerful organisation
- It has capacities that go beyond capacities of any non-state actor
- But even NATO cant break a simple encrypted file if it was encrypted by using a sophisticated password



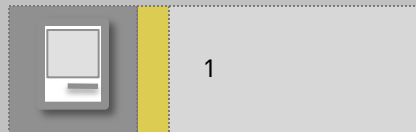
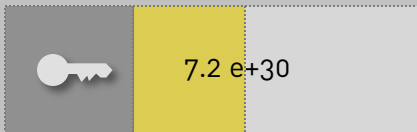
## 20 BIT ENCRYPTION



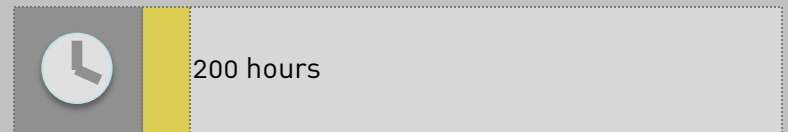
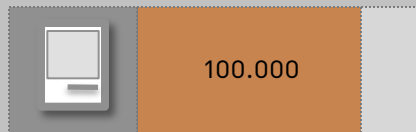
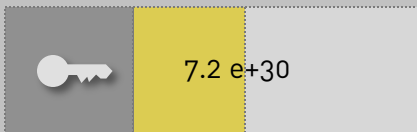
## 40 BIT ENCRYPTION



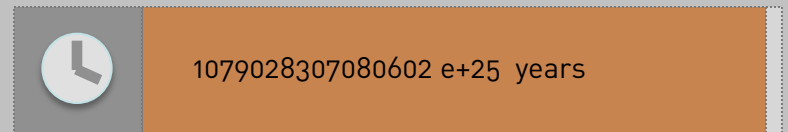
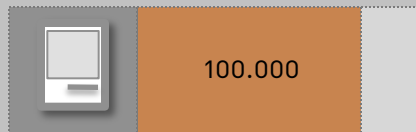
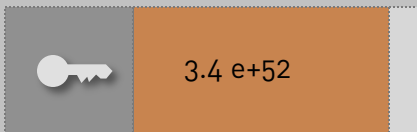
## 56 BIT ENCRYPTION



## 56 BIT ENCRYPTION



## 128 BIT ENCRYPTION



## MISSING CONTROL

- The military has developed advanced surveillance technology that allows them to intercept communication
- But this technology fails when it comes to simple things such as the interception of encrypted VoIP Communication



## ATTRIBUTION

- Military developed the most advanced ballistic missile early warning system
- It does not only to immediately detect and attack and prepare / prevent impact but also allows to detect the origin of an attack



## PREVIOUS INCIDENTS

- The attacks against Estonia were committed through a botnet
- Neither constitute an act of force nor did they take place during a conflict between two sovereign states
- Incidents during the conflict in Georgia in 2008 are the closest to being war-related
- The inability to determine the origin of the attacks as well as the fact that the discovered acts significantly differ from traditional warfare makes it difficult to characterise them as cyberwarfare



## PREVENTION


- Military is currently discussing advanced missile defence systems that are based on the most sophisticated technology (that is difficult to control)
- But they are most likely unable to prevent something as simple as a distributed denial of service attack



## CHALLENGES / CHANCES

## OPPORTUNITIES

- Case example 1: Within an investigation of a murder case law enforcement was unable to identify a murder based on search engine history. They were able to use search engine logs on the suspects computer to identify places he was interested in.

Article posted Nov 11 2005, 11:33 AM Category: [Big Brother/Orwellian](#) Source: [WRAL](#)  [Print](#)

### Man gets his Google search history submitted as evidence in murder trial

DURHAM, N.C. — Robert Petrick searched for the words "neck," "snap," "break" and "hold" on an Internet search engine before his wife died, according to prosecutors Wednesday.

More than two years after Janine Sutphen's body was discovered floating in a Raleigh lake, investigators continue to find new evidence on computers seized from Robert Petrick's home that prosecutors say support their arguments that Petrick killed his wife.

The Google search was the latest in recently discovered evidence found in the 100 million pages of content removed from computers.

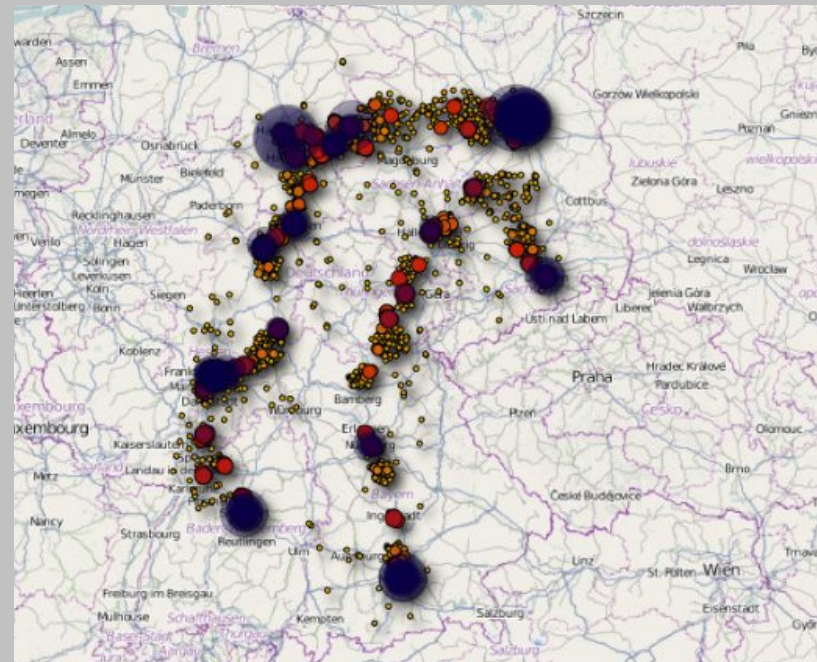
Last week, a forensic investigator discovered that Petrick allegedly researched lake levels, water currents, boat ramps and access about Falls Lake just four days before he reported Sutphen missing on Jan. 22, 2003.



Informationliberation.com

## DEVICES PROCESSING DATA

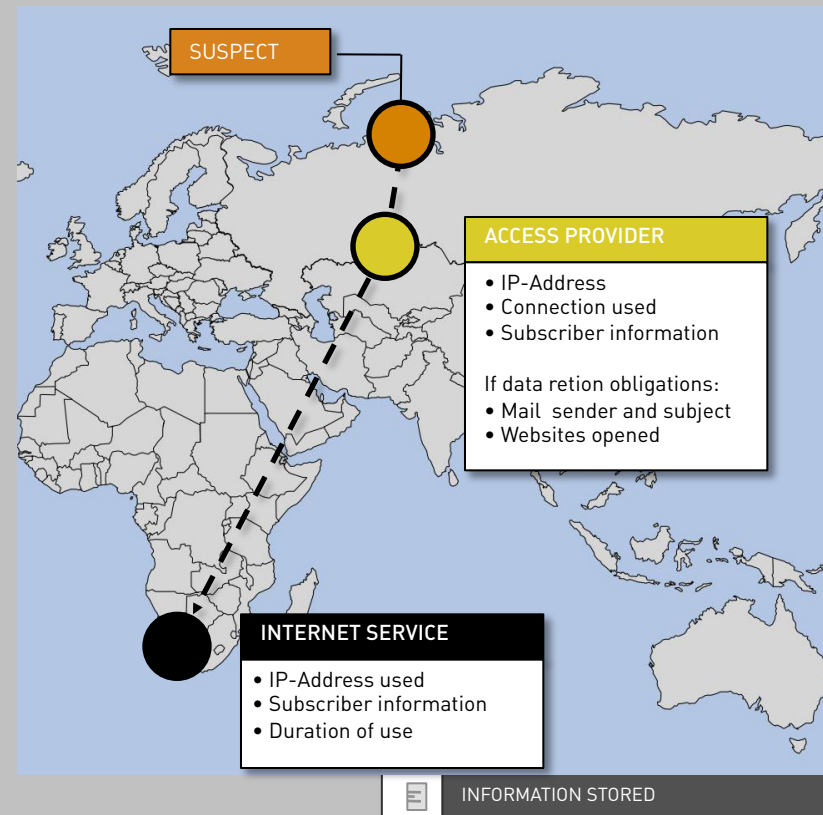
- Devices do often store information that are valuable for traditional investigation
- The user do not necessary have knowledge about such operation
- One example is the iPhone that stored the geo-location of the user and thereby enabled the reconstruction of movements/travel



EXAMPLE: AMAZON CLOUD COMPUTING

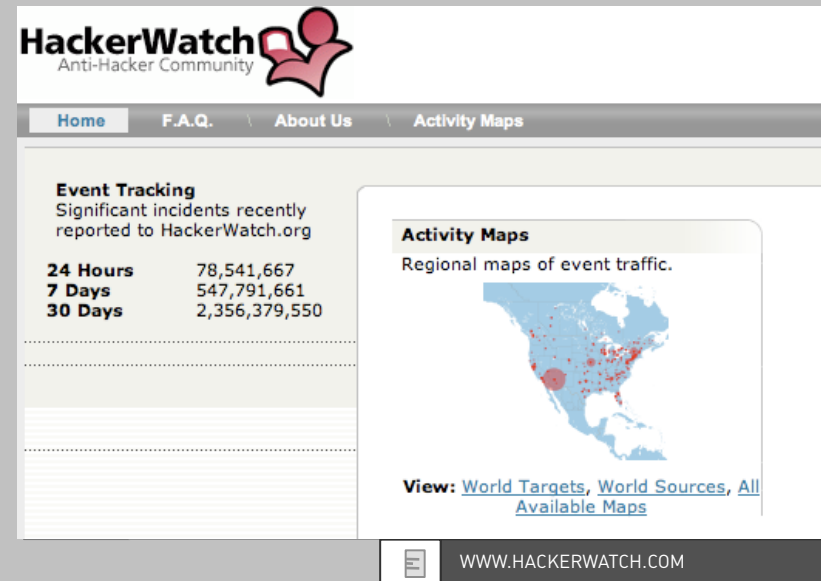
## TRACES

- “Nobody knows you are a dog” ?
- Internet users leave traces
- Access-Provider for example often for a certain period of time keep records to whom a dynamic IP-address was assigned
- Data retention obligations even increase the volume of data stored (but go along with questions related to the legality of this investigation instrument)



## AUTOMATE

- Computer and Networks enable offenders to automate attacks
- Within minutes millions of spam mails can be send out without generating high costs - sending out one million regular letters would be very expensive and take days
- The fact that millions of approaches to illegally enter a computer system are detected every day is not a result of the high number of offenders but the ability to automate attacks

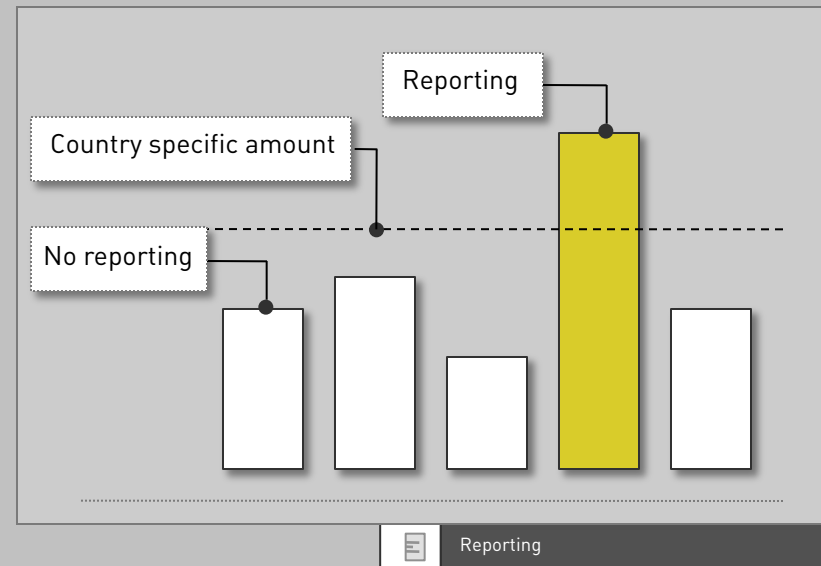


The screenshot displays the HackerWatch website, an Anti-Hacker Community. The page features a navigation menu with links for Home, F.A.Q., About Us, and Activity Maps. The main content area is divided into two sections: Event Tracking and Activity Maps. The Event Tracking section provides a summary of significant incidents reported to HackerWatch.org, with a table showing the number of incidents over different time periods. The Activity Maps section offers regional maps of event traffic, with a link to view world targets, world sources, and all available maps. The footer of the page includes the website's URL, WWW.HACKERWATCH.COM.

Time Period	Number of Incidents
24 Hours	78,541,667
7 Days	547,791,661
30 Days	2,356,379,550

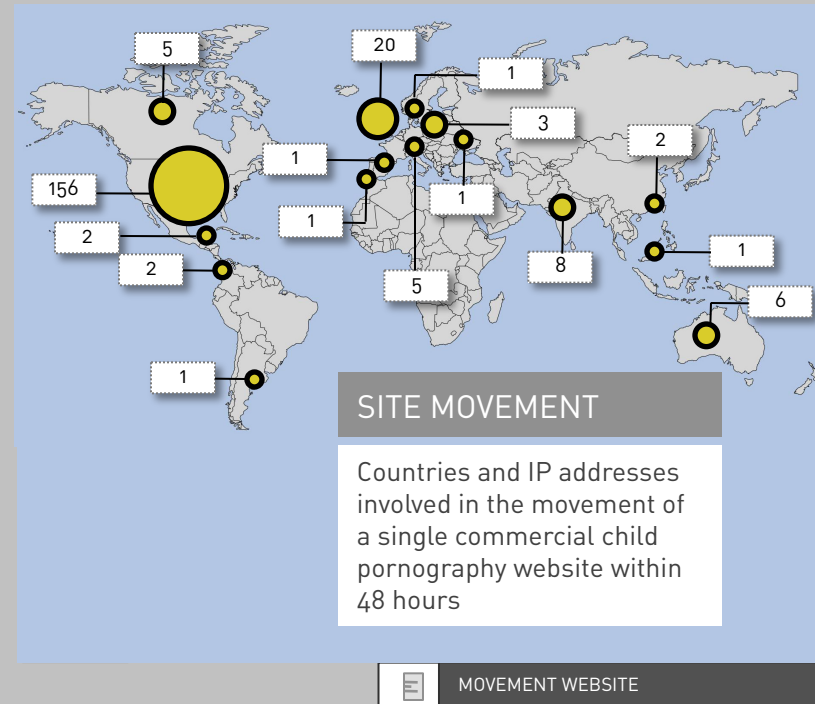
## AUTOMATE

- Automation enables offenders to generate high profit by committing various offences with rather small amounts each
- Background: Victims that have just lost rather small amounts tend not to report the crime



## SPEED OF DATA TRANSFER

- Data transfer speed enables quick move of data
- Offenders can make use of the speed of data transfer processes to hinder the removal of information



## WHAT HAPPENS IN THE REGION?

## HIPCAR

- In order to fight Cybercrime you need a comprehensive strategy
- This includes technology, officers, legislation, enforcement, ....
- HIPCAR is an EU/ITU funded project where 15 Caribbean countries developed several legal frameworks in the area of ICT – including Cybercrime
- Conceived by CARICOM and CTU
- Currently the most advanced legal framework in the world

## SPEED OF DATA TRANSFER

- Illegal Access
- Illegal Remaining
- Illegal Interception
- Illegal Data Interference
- Data Espionage
- Illegal System Interference
- Illegal Devices
- Computer-related Forgery
- Computer-related Fraud
- Child Pornography
- Identity-related crimes
- SPAM

## SPEED OF DATA TRANSFER

- Search and Seizure
- Assistance
- Production Order
- Expedited preservation
- Partial Disclosure of traffic data
- Collection of traffic data
- Interception of content data
- Forensic Software



**Cybercrime Research Institute**  
**Prof. Dr. Marco Gercke**

Niehler Str. 35  
D-50733 Cologne, Germany  
gercke@cybercrime.de  
[www.cybercrime-institute.com](http://www.cybercrime-institute.com)