

Киберсигурност

доц. д-р Златогор Минчев

E-mail: zlatogor@bas.bg



Част I - Въведение



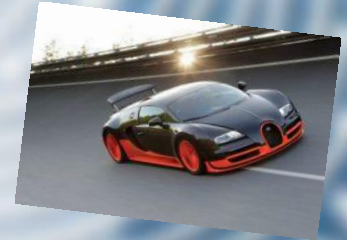
 **УчИМИ XI лятна изследователска школа по информатика**

Варна, България, 17-19 Юли, 2011

Съдържание

- Киберсвоят днес
- Какво е „киберсигурност“?
- Киберзаплахи
- Кибератаки
- Превенция на кибератаките

Киберсветът днес



Основни проблеми в съвременния киберсвят



- **Мащабността на технологичното развитие;**
- **Човеко-машинната комуникация;**
- **Човешкият фактор като източник на най-висока неопределеност и потенциална заплаха;**
- ...

Какво е „киберсигурност“?

„...Киберсигурността е съвкупност от методи и средства за откриване, защита и реакция на кибератаки в съответствие със съществуващите киберзаплахи и рискове за киберсвета...“, по разширена дефиниция на US-CERT, <http://www.us-cert.gov>

Киберзаплахи

**Зловреден софтуер
и измами**

**Интелигентни
среди**

Кибератаки

Зловреден софтуер и измами



- Зложелателен хардуер / Malicious Hardware
- Атаки срещу „облака“ / Attacks Against the Cloud
- Разширен зловреден софтуер / Advanced Malware
- Мобилен зловреден софтуер / Mobile Malware
- Рискове за информацията / Information Risks
- Насочени атаки / Targeted Attacks



Интелигентни среди

- Достъпност / Accessibility
- Системна сложност / System Complexity
- Поддръжка / Maintainability
- По-висока функционалност на устройствата /
More capable devices
- Мрежови слой на протоколи и услуги /
Network Layer Protocols and Services
- Повсеместни „четци“ / Ubiquitous Readers
- Атаки срещу компоненти различни от ICT /
Attacks against the non-ICT component





Кибератаките като киберзаплаха



- Уеб услуги и приложения / Web Services and Applications
- Критична инфраструктура / Critical Infrastructures
- Интелигентни, мобилни и многофункционални решения / Smart, Mobile and Ubiquitous Appliances
- Вътрешни агенти / Insiders
- Атаки срещу ядрото на мрежата / Network Core Attacks



Други кибератаки



- Атаки върху памети и техники на използване / **Memory Attacks**
- Атаки върху устройства / **Attacks on Devices**
- Отказ от услуги – **Denial of Services**
- Атаки в социалните мрежи и върху личността / **Social Networks & Privacy Attacks**
- Уеб атаки / **Web Attacks**
- Мрежови атаки / **Network level Attacks**
- Атаки във виртуални и облачни среди / **Virtualization & cloud Attacks**



Киберзаплахи в ICT инфраструктурата

forward»

Managing Emerging Threats in ICT Infrastructures



FORWARD is an initiative by the European Commission (under FP7) to promote the collaboration and partnership between Academia and Industry in their common goal of protecting Information and Communication Technology (ICT) infrastructures.

Основен резултат:

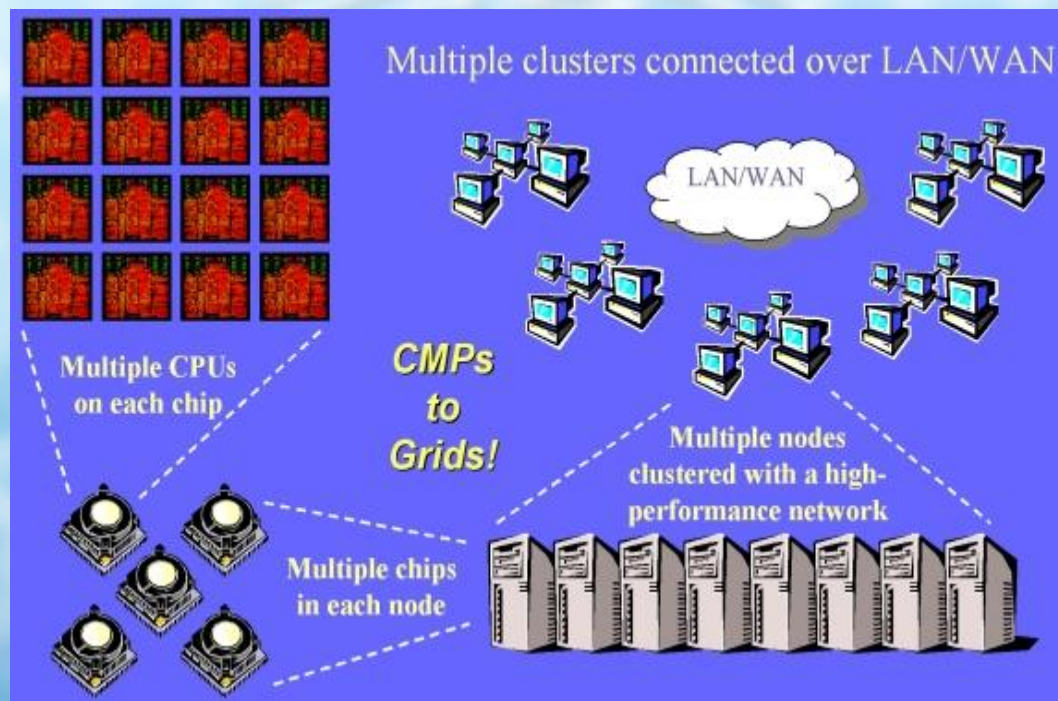
FORWARD Whitebook: Emerging ICT Threats



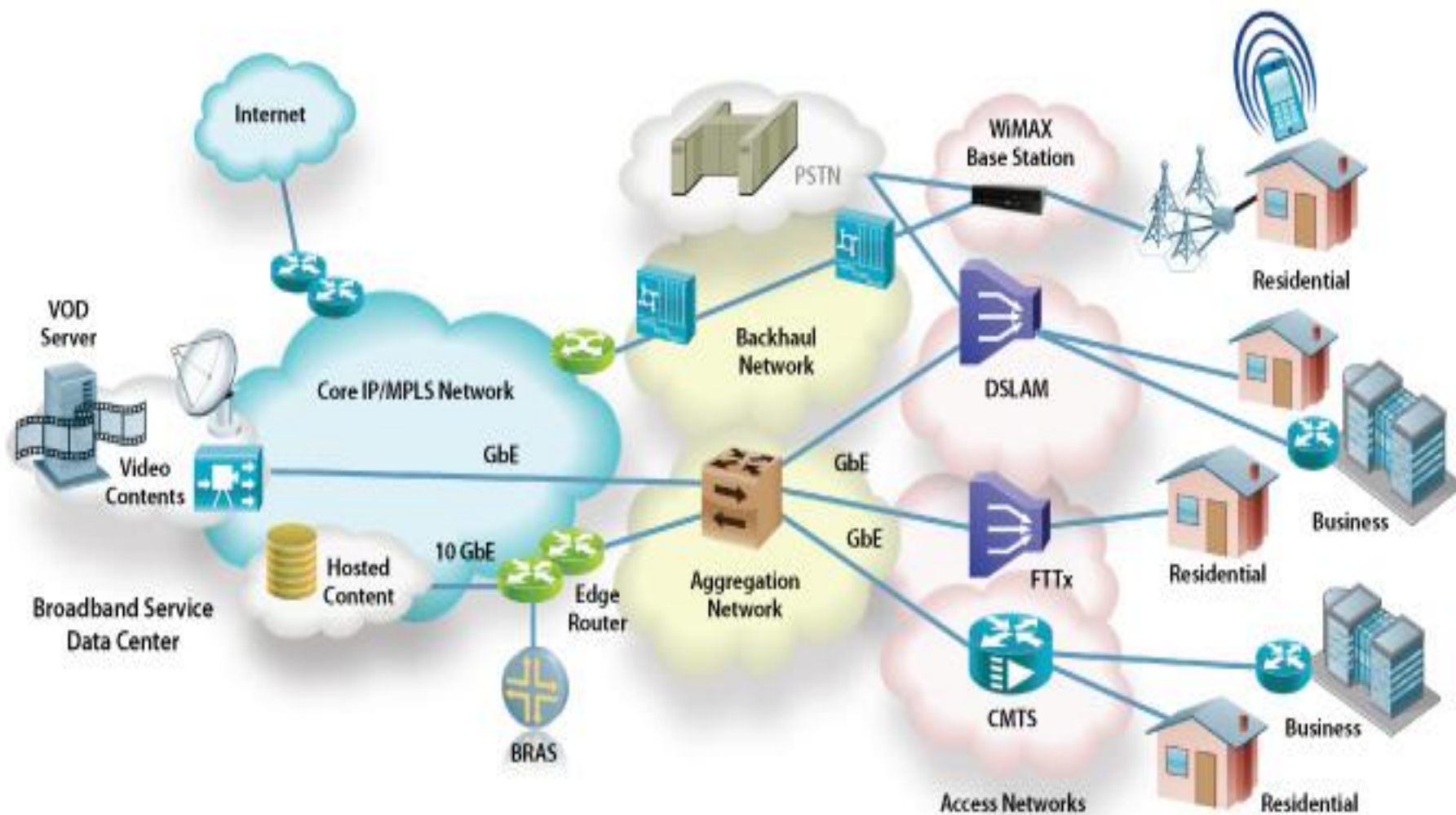
Списък на възможни бъдещи киберзаплахи

#	Threat Description	High Priority			
		Impact	Likely	Oblivious	R&D
1	Threats due to parallelism	M	M	H	M
2	Threats due to scale	H	M	H	M
3	Underground economy support structures	H	H	L	H
4	Mobile device malware	H	H	M	H
5	Threats related to social networks	H	H	M	H

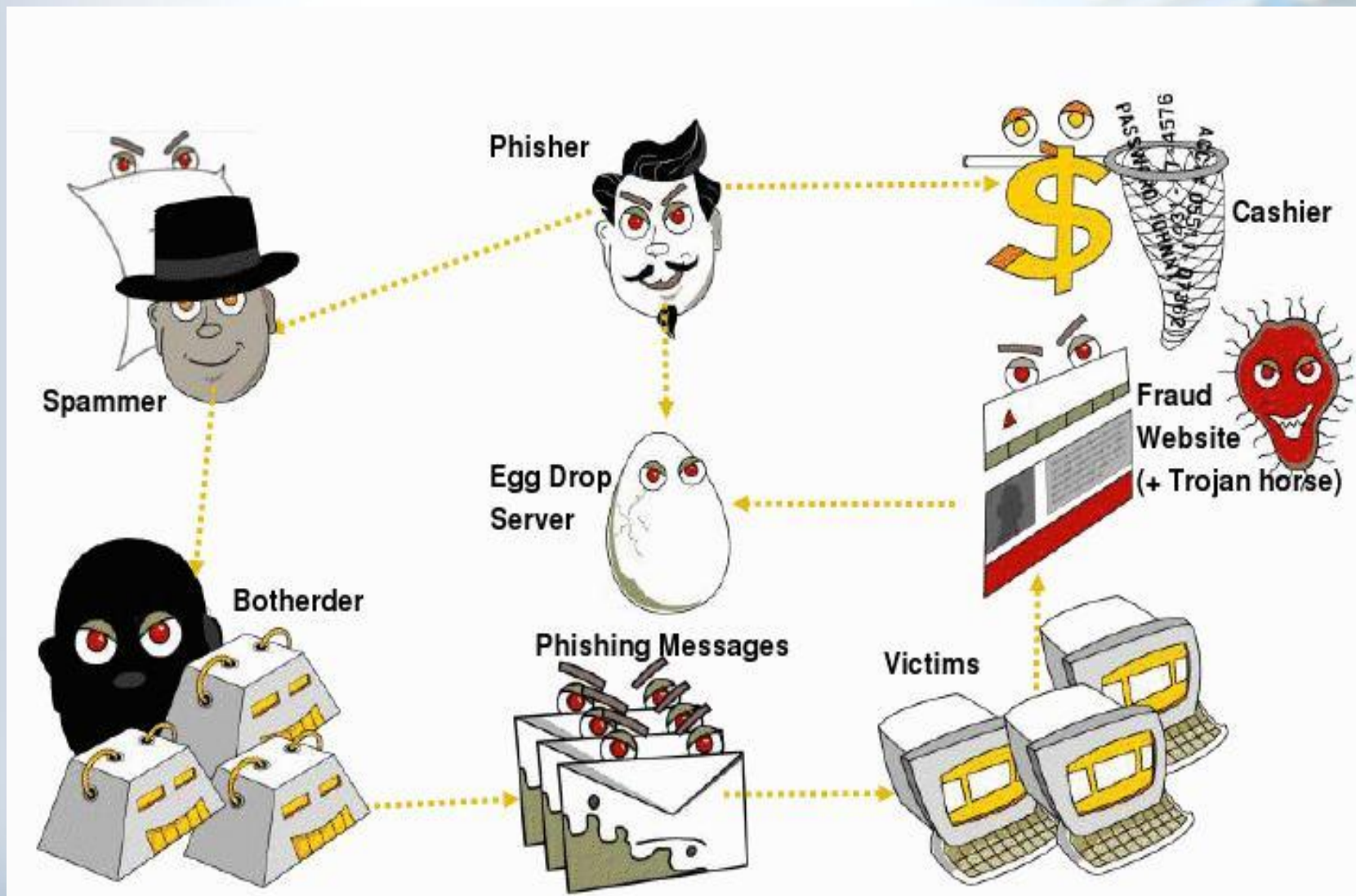
Заплахи заради паралелизма



Заплахи заради мащаба

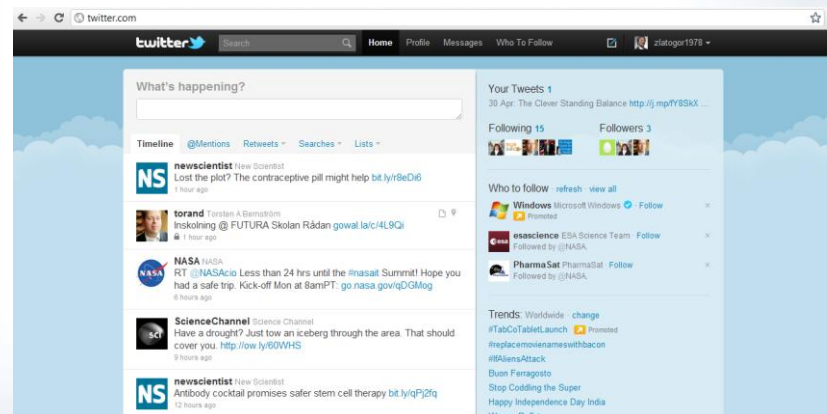
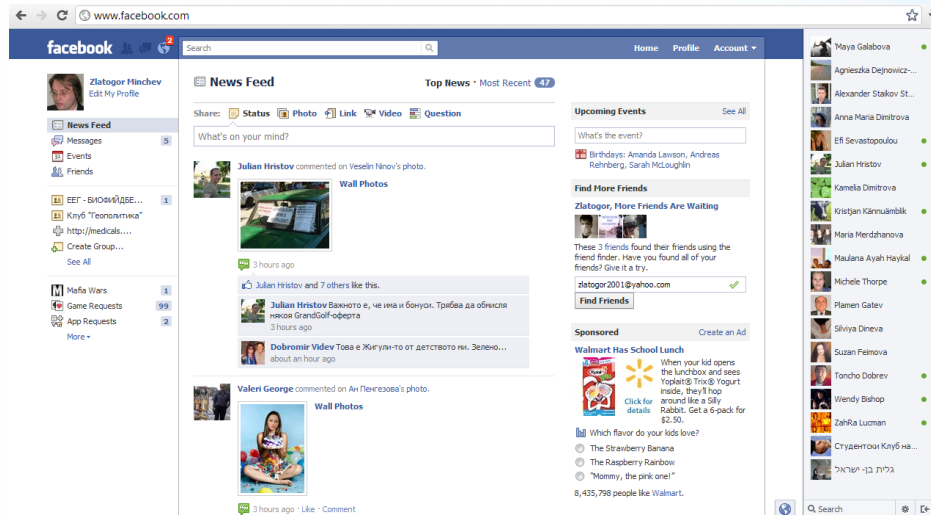


Поддържащи структури на икономика на подземен свят





Заплахи свързани със социалните мрежи



http://en.wikipedia.org/wiki/List_of_social_networking_websites

Medium Priority					
#	Threat Description	Impact	Likely	Oblivious	R&D
6	Routing infrastructure	H	H	L	M
7	Denial of service	H	H	L	M
8	Wireless communication	H	H	M	M
9	Unforeseen cascading effects	H	M	H	H
10	False sensor data	H	M	H	M
11	Privacy and ubiquitous sensors	M	M	M	M
12	User interface	M	H	M	H
13	The insider threat	H	M	M	M
14	System maintainability and verifiability	M	H	M	M
15	Hidden functionality	M	M	H	M
16	New vectors to reach victims	M	H	M	H
17	Sensors and RFID	M	H	M	H
18	Advanced malware	M	H	M	M
19	Virtualization and cloud computing	H	M	H	M
20	Retrofitting security to legacy systems	M	M	M	L
21	Next generation networks	H	H	M	M

Low Priority					
#	Threat Description	Impact	Likely	Oblivious	R&D
22	IPv6 and direct reachability of hosts	M	H	M	M
23	Naming (DNS) and registrars	L	H	M	L
24	Online games	L	H	M	L
25	Safety takes priority over security	L	M	H	M
26	Targeted attacks	M	H	M	M
27	Malicious hardware	M	L	H	M
28	Use of COTS components	M	H	M	M

10 сценария върху заплахите в ICT инфраструктурата

- **Election Fraud**
- **Crashing the Stock Market for Fun & Profit**
- **Industrial Espionage**
- **The Smart Grid**
- **The Oil Spill**
- **Fabrication Take Over**
- **The Politician's Phone**
- **Mass Blackmailing through Social Networks**
- **Attack Against an Electric Power Station**
- **Attack on a Water Power Station**

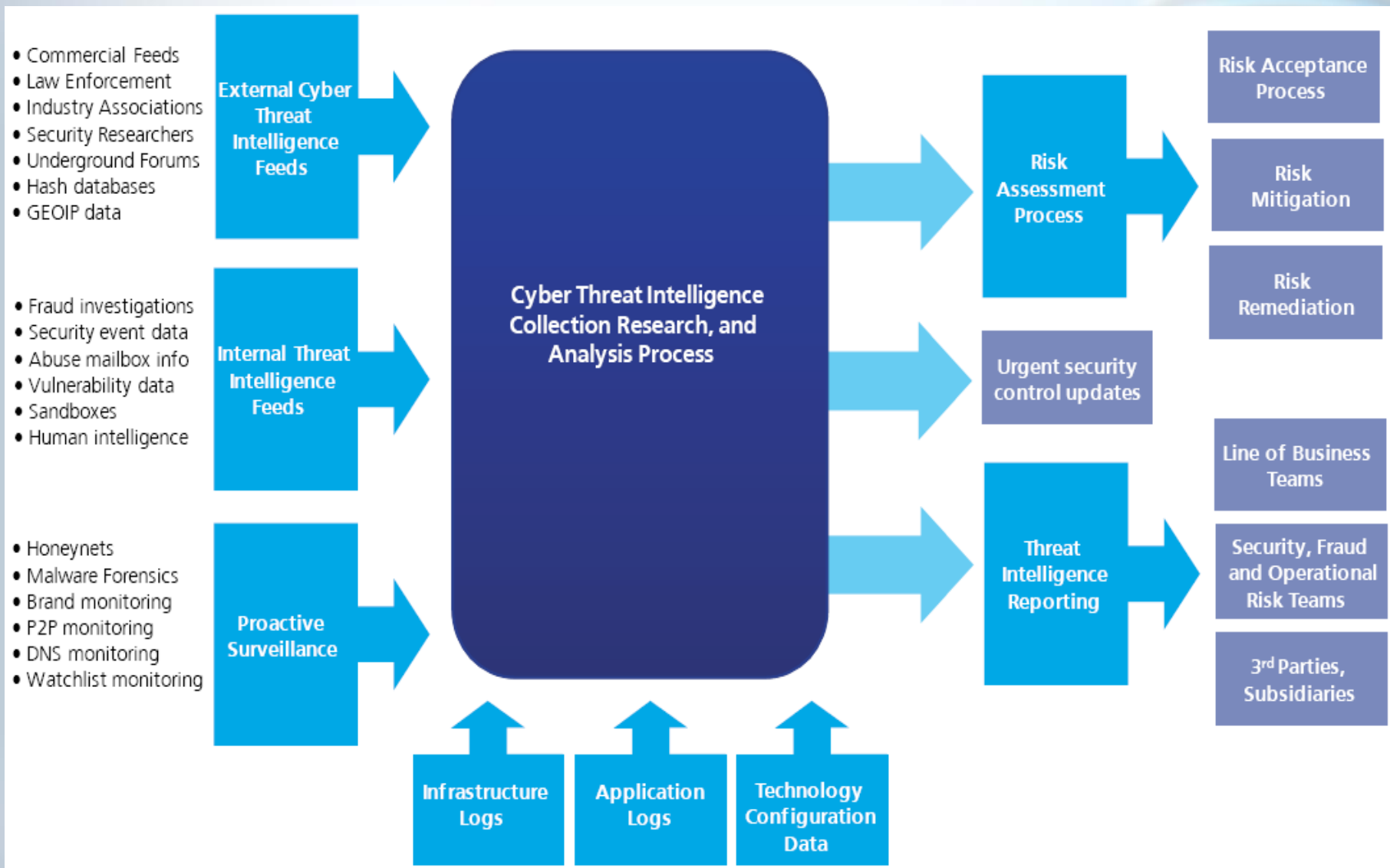
Някои нови приоритетни киберзаплахи

Threat-Enabler \ Assets	Personal Assets				Societal Assets		Professional Assets
	Privacy (Human Rights)	Digital Identity	Financial Assets	Health Safety	Critical Infrastructures	GRIDS Clouds	Data Sales etc.
Anonymous Internet Access	Medium	Medium	Low	Low	Medium	Low	Medium
Ubiquitous networks	High	High	High	High	Low	Low	Low
Human Factors	High	High	High	High	High	High	High
Insider attacks	High	High	High	High	High	High	High
Botnets	High	High	High	High	High	High	High
Program Bugs	High	High	High	High	High	High	High
Scale and Complexity	High	High	High	High	High	High	High
Mobile Devices	High	High	High	High	Medium	Low	High
24/7 connectivity	High	High	High	High	Low	Low	High
more private info available	High	High	Medium	High	Low	Low	Low
smart meters	High	High	Medium	High	High	Low	Low
Tracking	High	High	Medium	High	Low	Low	High
Smart Environments	High	High	Medium	High	Medium	Low	High
Unsecured Devices	High	High	High	High	Low	Low	High
Social networks	High	High	Medium	Medium	Low	Low	Low
Cyber-physical connectivity for Infrastructures, cars etc.	High	Low	Medium	High	High	Low	High
Organized Cyber Crime	High	High	High	High	High	Low	High
Mobile Malware	High	High	High	High	Medium	Low	High
SCADA Malware	Low	Low	Low	Low	High	Low	Medium
	Privacy (Human Rights)	Digital Identity	Financial Assets	Health Safety	Critical Infrastructures	GRIDS Clouds	Data Sales etc.

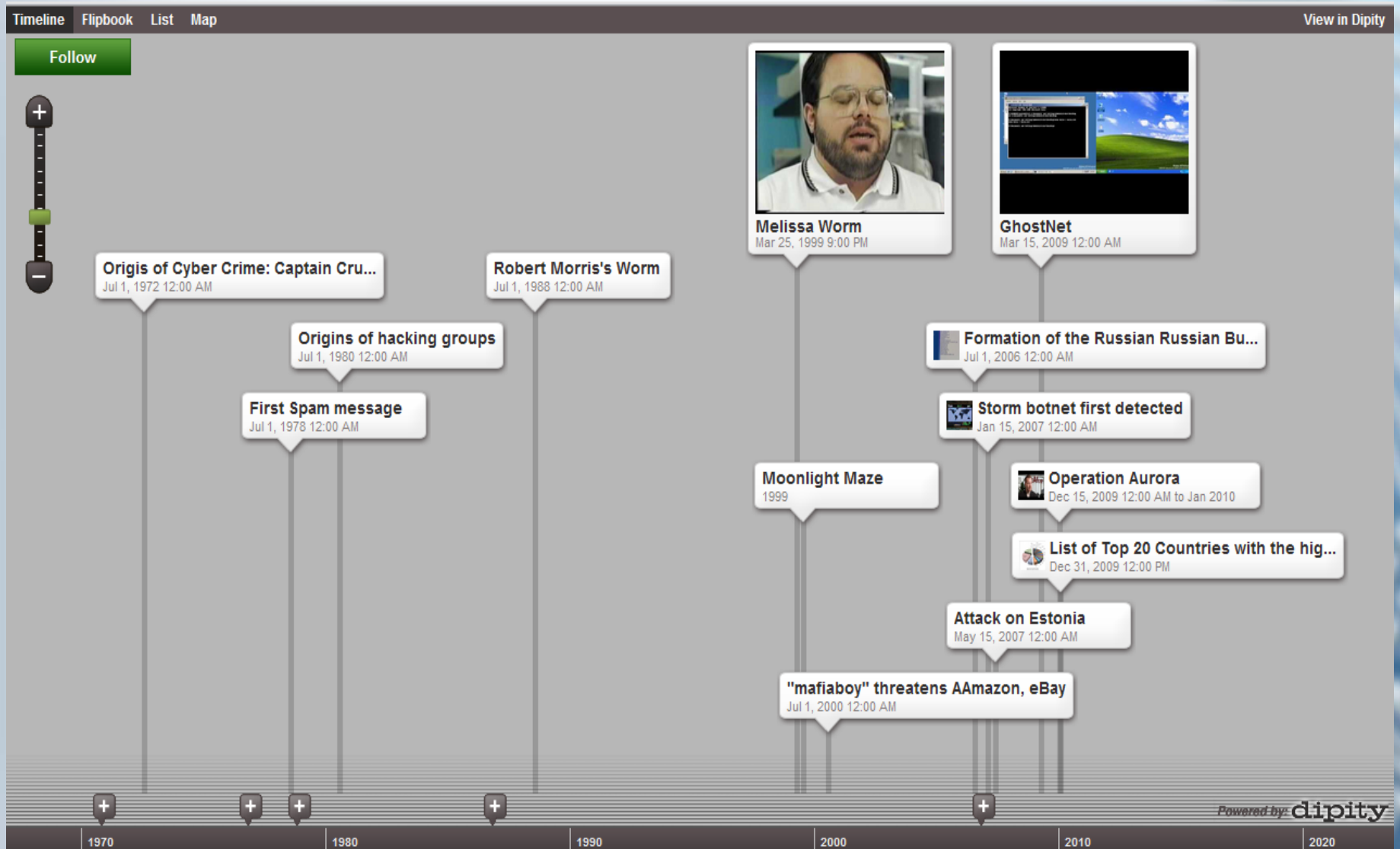
Сценарии за бъдещи киберзаплахи

- Атака върху банковите сметки на частно лице използващо интелигентни мобилни устройства и персонален компютър;
- Атака върху интелигентни измервателни устройства с участието на организирана престъпна група.

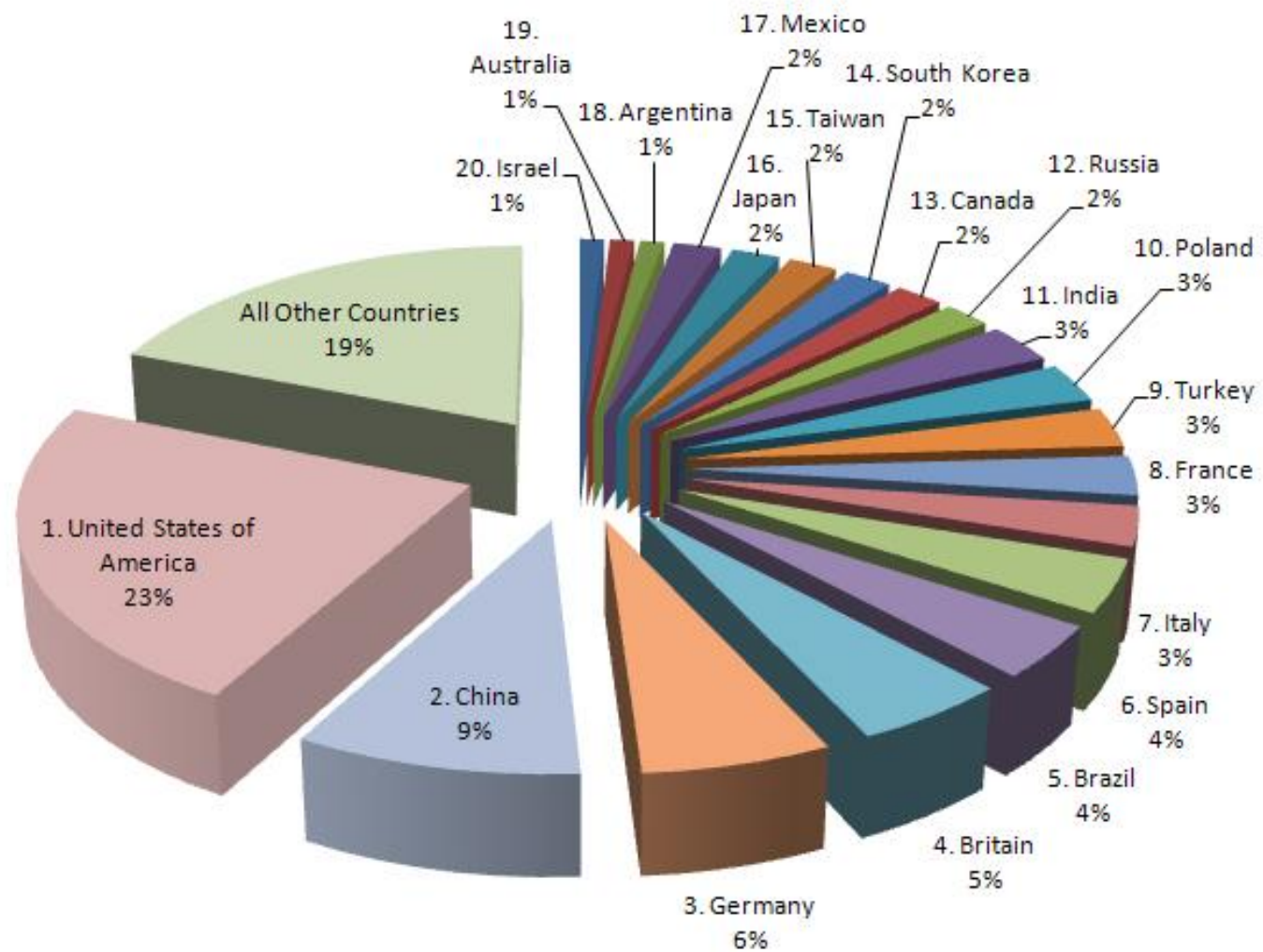
Превенция на кибератаките



Киберпреступления



<http://www.dipity.com/priyankalakhe/A-history-of-Cyber-crime-and-warfare/>



Cybercrime: Top 20 Countries

EU Cybercrime Task Force

[←](#) [→](#) [↻](#) [www.europol.europa.eu/index.asp?page=news&news=pr100622.htm](#) [☆](#)

bg cs da de el en es et fi fr hu it lt lv mt nl pl pt ro sk sl sv

04 April 2011



EUROPOL > Press Room > Press Releases

[F.A.Q.](#) [Search](#) [Links](#) [Site Map](#) [Disclaimer](#)

[Home](#)
[Europol Overview](#)
[Publications](#)
[Management](#)
[Legal](#)
[Press Room](#)
[Job Opportunities](#)
[Internships](#)
[Procurement](#)
[Contact us](#)

The Hague, 22 June 2010

European Union Cybercrime Task Force

The Hague - The Netherlands.

The creation of a European Union Cybercrime Task Force is the result of a two-day meeting held at Europol Headquarters on 14 and 15 June 2010. The meeting was attended by the Heads of European Union Cybercrime Units and representatives from Eurojust and the European Commission. Under discussion were operational and strategic issues on cybercrime investigations, prosecutions and cross-border cooperation in the fight against cybercrime.

Subjects like cross-border operational info-exchange, cybercrime case studies, new criminal trends, criminal modus operandi, international legal constraints, relationship with private industries, negotiation with non-European Union law enforcement organisations, and training of law enforcement were all discussed during the event.

A specific session was dedicated to the establishment of the so-called European Cybercrime Platform that includes the Internet Crime Reporting Online System (ICROS), the Analysis Work File Cyborg, that is actively working to fight criminal groups operating on the internet, and the Internet & Forensic Expert Forum (IFOREX) to host technical data and training for cybercrime law enforcement. The Platform is a first step towards a more consistent and effective approach to fighting internet criminality at EU level.

Current EU-Presidency:
Hungary
[www.eu2011.hu](#)

The European Union
online:
[www.europa.eu](#)

Joint Investigation
Teams
[www.europol.europa.eu](#)

INTERPOL
[www.interpol.int](#)

Be smart with your card
[www.europol.europa.eu](#)

USDJ Computer Crime & IP Section

← → ↻ www.cybercrime.gov ☆



Computer Crime & Intellectual Property Section United States Department of Justice

Home Computer Crime Intellectual Property Electronic Evidence Other High Tech Legal Issues About CCIPS

News Site Index Search

Computer Crime & Intellectual Property Section

Latest Press Releases

- Former Milford Man Charged with Conspiracy to Commit Copyright Infringement (March 29, 2011)
- Five Domestic Defendants Linked to International Computer Hacking Ring Guilty of Federal Fraud Charges: 46 People Charged in Operation 'Phish Phry' Have Now Been Convicted (March 25, 2011)
- Chinese Counterfeit Perfume Importers Indicted for Allegedly Trafficking in Counterfeit Goods (March 23, 2011)
- Bakersfield Business Owner Indicted for Trafficking in Counterfeit Goods (March 21, 2011)
- Former Goldman Sachs Computer Programmer Sentenced to 97 Months in Prison for Stealing Firm's Trade Secrets (March 18, 2011)
- Former Security Guard, Who Hacked into Hospital's Computer System, Is Sentenced to 110 Months in Federal Prison (March 18, 2011)
- Tyngsboro Company Charged with Selling Counterfeit Computer Equipment (March 18, 2011)
- Montgomery County Police Officer Charged with Drug Trafficking Conspiracy and Computer Fraud (March 16, 2011)
- New York Man Pleads Guilty to Federal Copyright Violation for Illegally Uploading Copy of X-Men Movie (March 14, 2011)
- Former Société Générale Trader Sentenced in Manhattan Federal Court to 36 Months in Prison for Stealing Bank's Trade Secrets (February 28, 2011)
- International Computer Hacker Sentenced to 82 Months in Prison (February 28, 2011)
- Lithonia Woman Indicted for Computer Fraud Using IRS Computers (February 28, 2011)
- Seven Members of Romanian Organized Crime Group Charged in International Wire Fraud Scheme (February 25, 2011)

Hot Documents

- **How to Report Cyber and IP Crime**
 - [How to Report Computer- and Internet-Related Crime](#)
 - [How to Report Intellectual Property Crime](#)
- IP Enforcement Coordinator's 2010 Annual Report (February 2011)
- PRO IP Act Annual Report 2010 (PDF) (December 2010)
- FBI PRO IP Act Annual Report 2010 (PDF) (December 2010)
- 2010 Joint Strategic Plan on Intellectual Property Enforcement(PDF) (June 2010)
- Testimony of Deputy Assistant Attorney General Jason M. Weinstein on Combating IP Crime (PDF) (December 2009)
- USA Bulletin on Economic Espionage and Trade Secrets (PDF) (November 2009)
- CCIPS Manual on Electronic Search and Seizure - Updated 2009 (August 24, 2009)
- New Law Review Article, "Data Breaches: What the Underground World of 'Carding' Reveals"(PDF) (May 2008)
- NPR Interview with CCIPS and FBI: Cyber Sleuths Zero In as Web Fraud Takes Toll (January 20, 2008)
- Digital Forensic Analysis Methodology Flowchart (PDF) (August 22, 2007)
- CCIPS "Prosecuting Computer Crimes" Manual (March 2007)
- CCIPS "Prosecuting Intellectual Property Crimes" Manual (October 2006)

Български портал на МВР „Cyber Crime“

[←](#) [→](#) [↺](#) [www.cybercrime.bg/bg](#) [★](#) [🔧](#)



[Начало](#) | [Карта на сайта](#) | [Контакти](#)

CyberCrime

Официален сайт за борба с компютърните престъпления



Стеник Груп ООД
Официален партньор

[Подай сигнал
за извършено компютърно престъпление](#)



Какво е ФИШИНГ и как да се предпазим от него? Кои са другите дигитални заплахи в ИНТЕРНЕТ, как да ги разпознаваме и неутрализираме? [[Научи повече](#)]



Защитени ли са децата ни в глобалната мрежа? Какво трябва да знаят децата и техните родители за безопасното използване на интернет! [[Научи повече](#)]

Интернет заплахи

Експлоатация на деца

Цели на сайта

Целта на този уебсайт е да предостави полезна информация при борбата с компютърни престъпления, фишинг, сексуална експлоатация на деца, престъпления срещу интелектуалната собственост и незаконен хазарт. Тук можете да откриете отговори как да процедурите ако интернет сайта[...]

[Прочети повече](#)

Новини

Обща кампания срещу онлайн кражбата на съдържание
08.07.2011

Интернет доставчиците и творческите организации стартират обща кампания[...]

► [Прочети цялата новина](#)

[1](#) [2](#) [3](#)

 [Архив новини](#)

Последно видео

[Всички клипове](#)



0:00 / 0:00

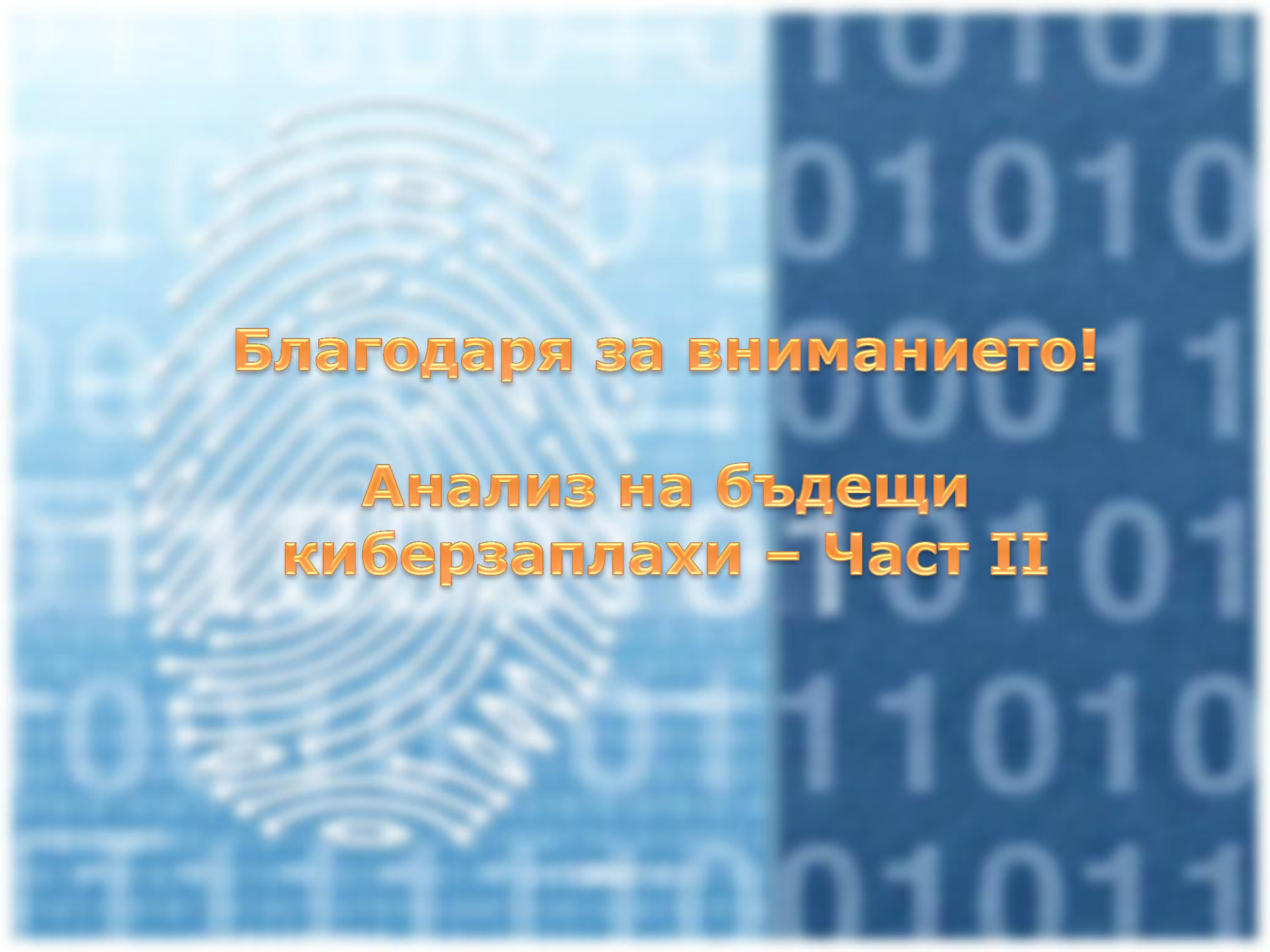
Академични активности в областта на киберсигурността

**A European Network of Excellence in Managing Threats and
Vulnerabilities in the Future Internet:
Europe for the World, EU FP7**

SySSec 2010 -2014



... Instead of reactively chasing after attackers,
we should start working proactively and think
about emerging threats and vulnerabilities...



Благодаря за вниманието!

**Анализ на бъдещи
киберзаплахи – Част II**

Киберсигурност

доц. д-р Златогор Минчев

E-mail: zlatogor@bas.bg



Част II - Анализ на бъдещи киберзаплахи



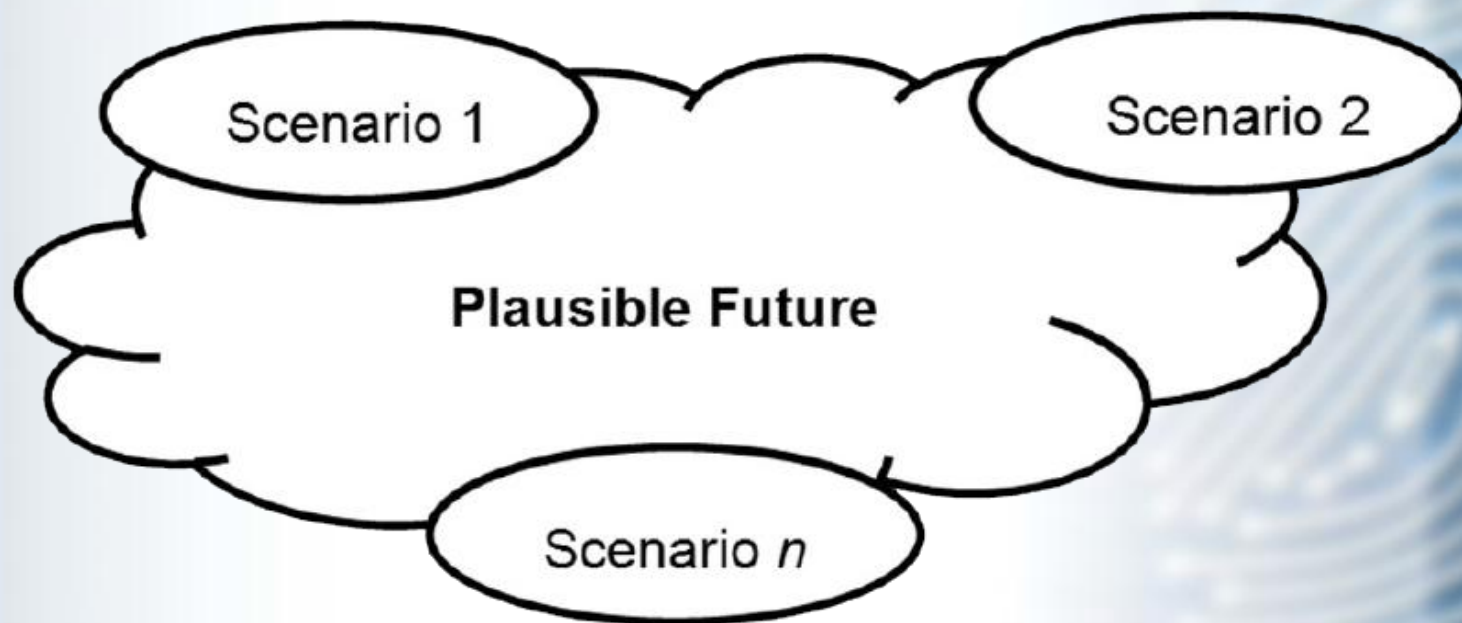
УчИМИ XI лятна изследователска школа по информатика

Варна, България, 17-19 Юли, 2011

Съдържание

- **Метод на сценариите**
- **Морфологичен анализ**
- **Системен анализ**
- **Валидиране на резултатите**
- **Модел на информационните потоци в социалната мрежа Facebook**

Метод на сценариите



Събиране на експертни знания

- Мозъчна атака (генериране на базови идеи);
- Модифициран Delphi метод (филтриране на резултатите);

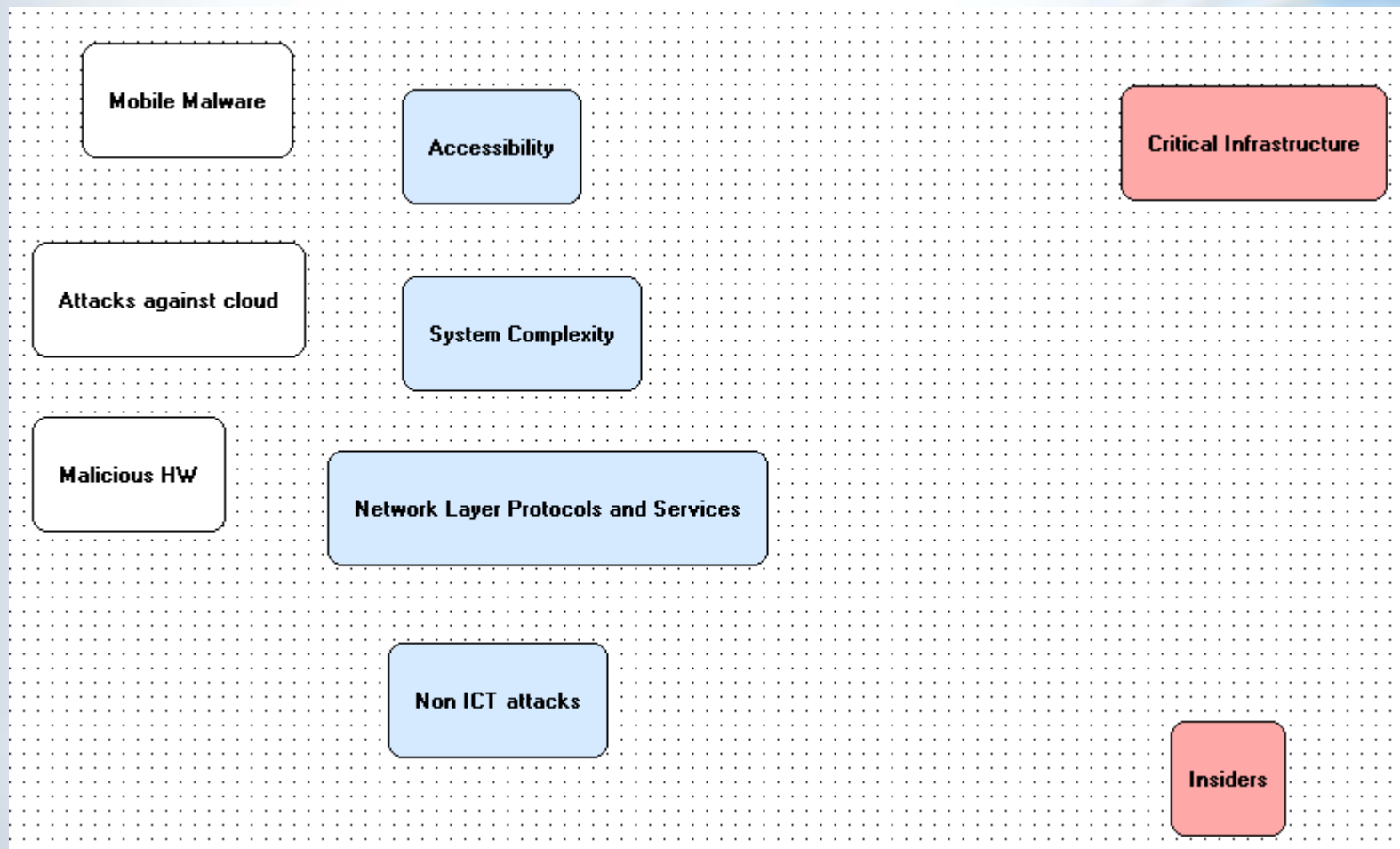
Събиране на експертни знания

- **Техники:**
 - Морфологичен (структурен) анализ;
 - Системен анализ;
- **Помощни софтуерни среди:**
 - MS Office®/OpenOffice; • Final Draft®
 - Intelligent Scenario Computer Interface Program (I-SCIP®).

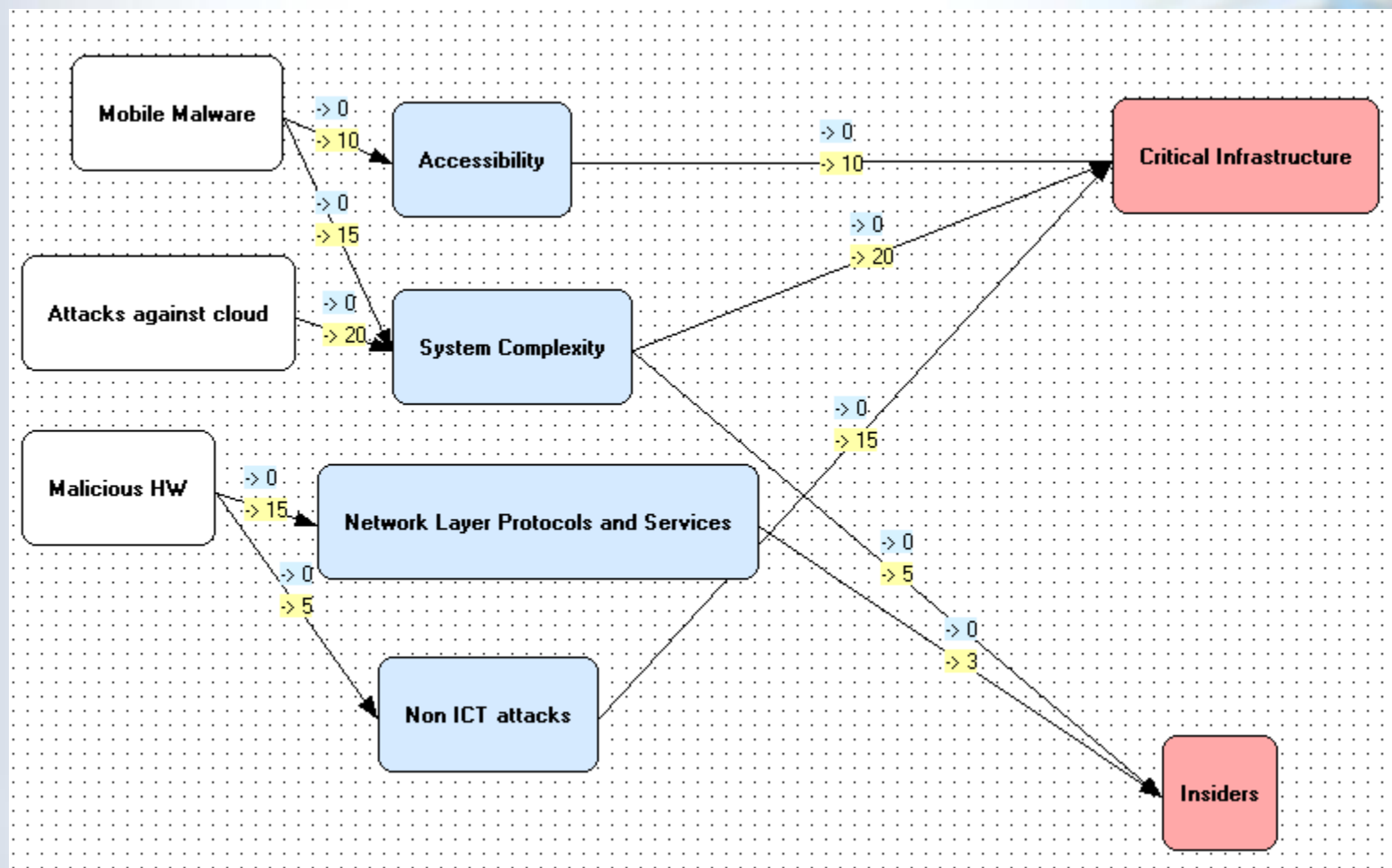
Морфологичен анализ

- Пълно разглеждане на задачата;
- Широко използване в класификационни задачи;
- Познат и разпространен в научно-изследователската област метод.

Стъпка 1: Дефиниране на размерности и алтернативи



Стъпка 2: Свързване на алтернативи



Матрица на конфликтите / матрица на кросконсистентност

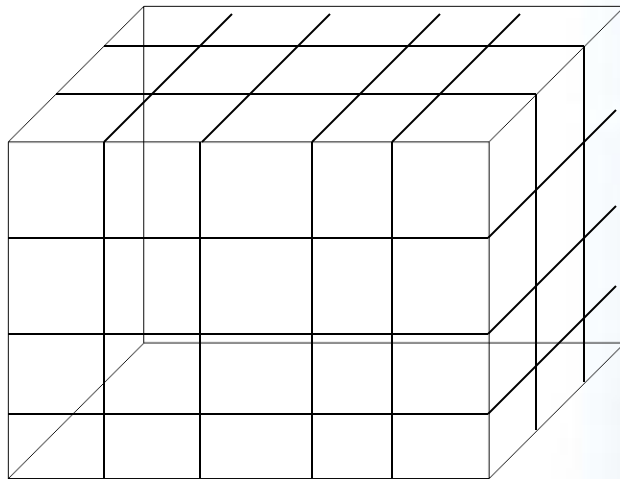
Морфологичен анализ

Malware and Fraud	Smart Environments	Cyberattacks
Mobile Malware	Accessibility	Critical Infrastructure
Attacks against cloud	System Complexity	Insiders
Malicious H/W	Network Layer Protocols and Services	
	Non ICT attacks	

Индекс	Дължина	Тегло	Име	
1	3	20		Активни сценарии + Пасивни сценарии -
2	3	20		
3	3	25		
4	3	18		
5	3	20		
6	3	35		
7	3	40		

Общ обем на задачата

Възможни комбинации: $3 \times 4 \times 2 \times 3 = 72$



Стъпка 3: Генериране на сценарии, подреждане и именуване

Морфологичен анализ		
Malware and Fraud	Smart Environments	Cyberattacks
Mobile Malware	Accessibility	Critical Infrastructure
Attacks against cloud	System Complexity	Insiders
Malicious HW	Network Layer Protocols and Services	
	Non ICT attacks	

Индекс	Дължина	Тегло	Име
1	3	20	Scenario1
2	3	20	Scenario2
3	3	25	Scenario3
4	3	18	Scenario4
5	3	20	Scenario5
6	3	35	Scenario6
7	3	40	Scenario7

Активни сценарии +



Пасивни сценарии -

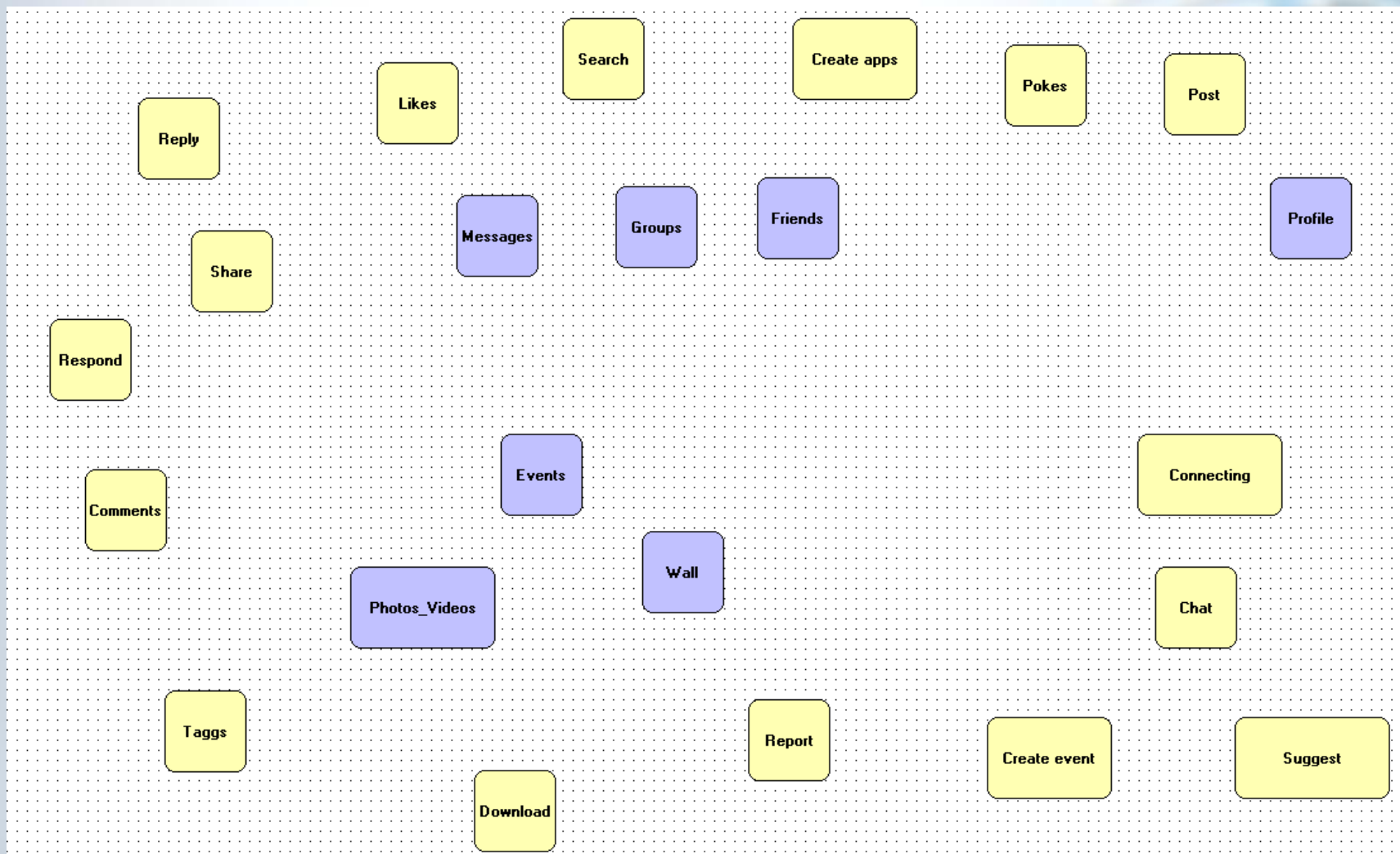
Някои нови приоритетни киберзаплахи

Threat-Enabler \ Assets	Personal Assets				Societal Assets		Professional Assets
	Privacy (Human Rights)	Digital Identity	Financial Assets	Health Safety	Critical Infrastructures	GRIDS Clouds	Data Sales etc.
Anonymous Internet Access	Medium	Medium	Low	Low	Medium	Low	Medium
Ubiquitous networks	High	High	High	High	Low	Low	Low
Human Factors	High	High	High	High	High	High	High
Insider attacks	High	High	High	High	High	High	High
Botnets	High	High	High	High	High	High	High
Program Bugs	High	High	High	High	High	High	High
Scale and Complexity	High	High	High	High	High	High	High
Mobile Devices	High	High	High	High	Medium	Low	High
24/7 connectivity	High	High	High	High	Low	Low	High
more private info available	High	High	Medium	High	Low	Low	Low
smart meters	High	High	Medium	High	High	Low	Low
Tracking	High	High	Medium	High	Low	Low	High
Smart Environments	High	High	Medium	High	Medium	Low	High
Unsecured Devices	High	High	High	High	Low	Low	High
Social networks	High	High	Medium	Medium	Low	Low	Low
Cyber-physical connectivity for Infrastructures, cars etc.	High	Low	Medium	High	High	Low	High
Organized Cyber Crime	High	High	High	High	High	Low	High
Mobile Malware	High	High	High	High	Medium	Low	High
SCADA Malware	Low	Low	Low	Low	High	Low	Medium
	Privacy (Human Rights)	Digital Identity	Financial Assets	Health Safety	Critical Infrastructures	GRIDS Clouds	Data Sales etc.

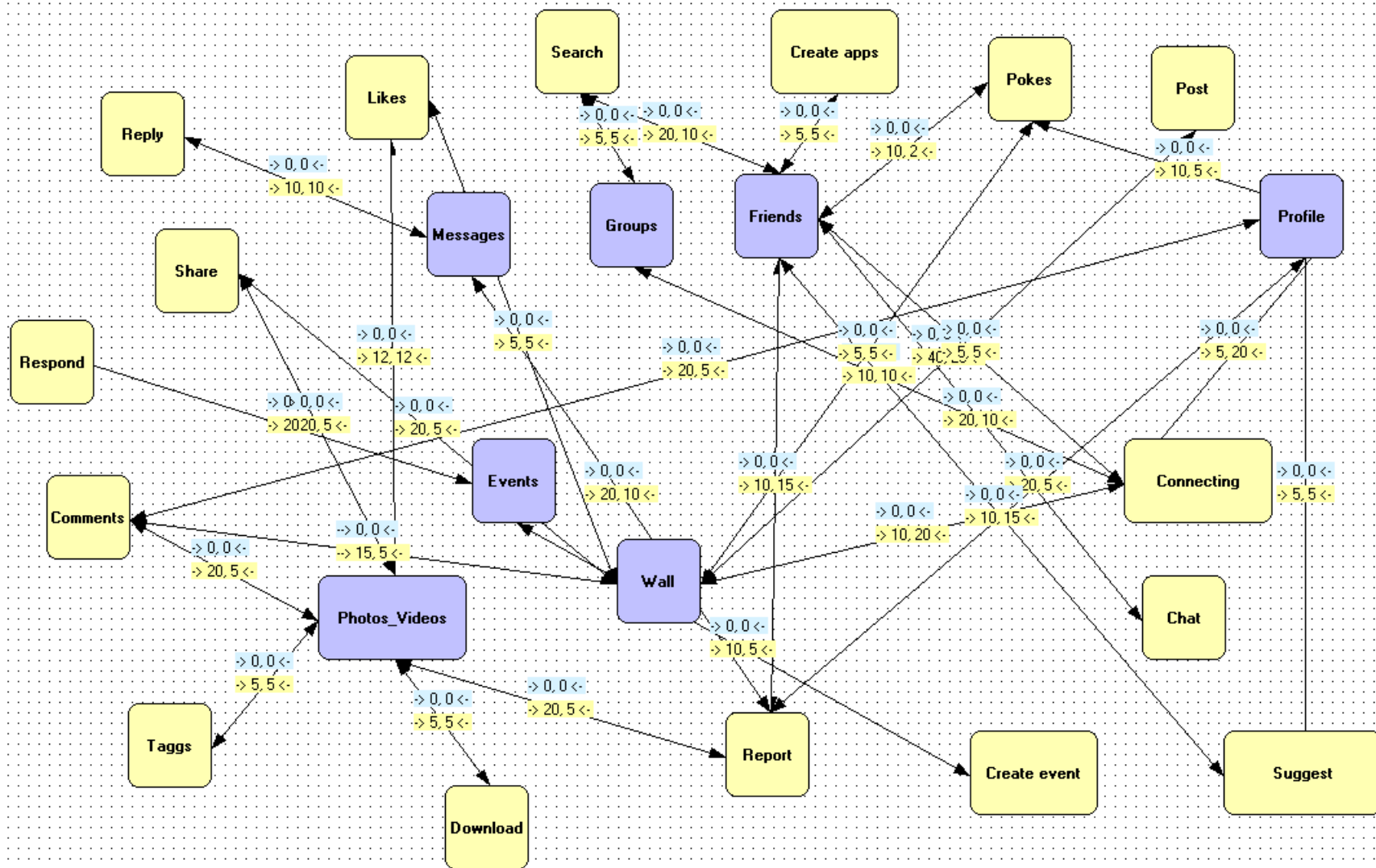
Системен анализ

- Използване на машинно представяне от типа „обект връзка“;
- Разглеждане на детайлите;
- Познат и разпространен в научно-изследователската област метод.

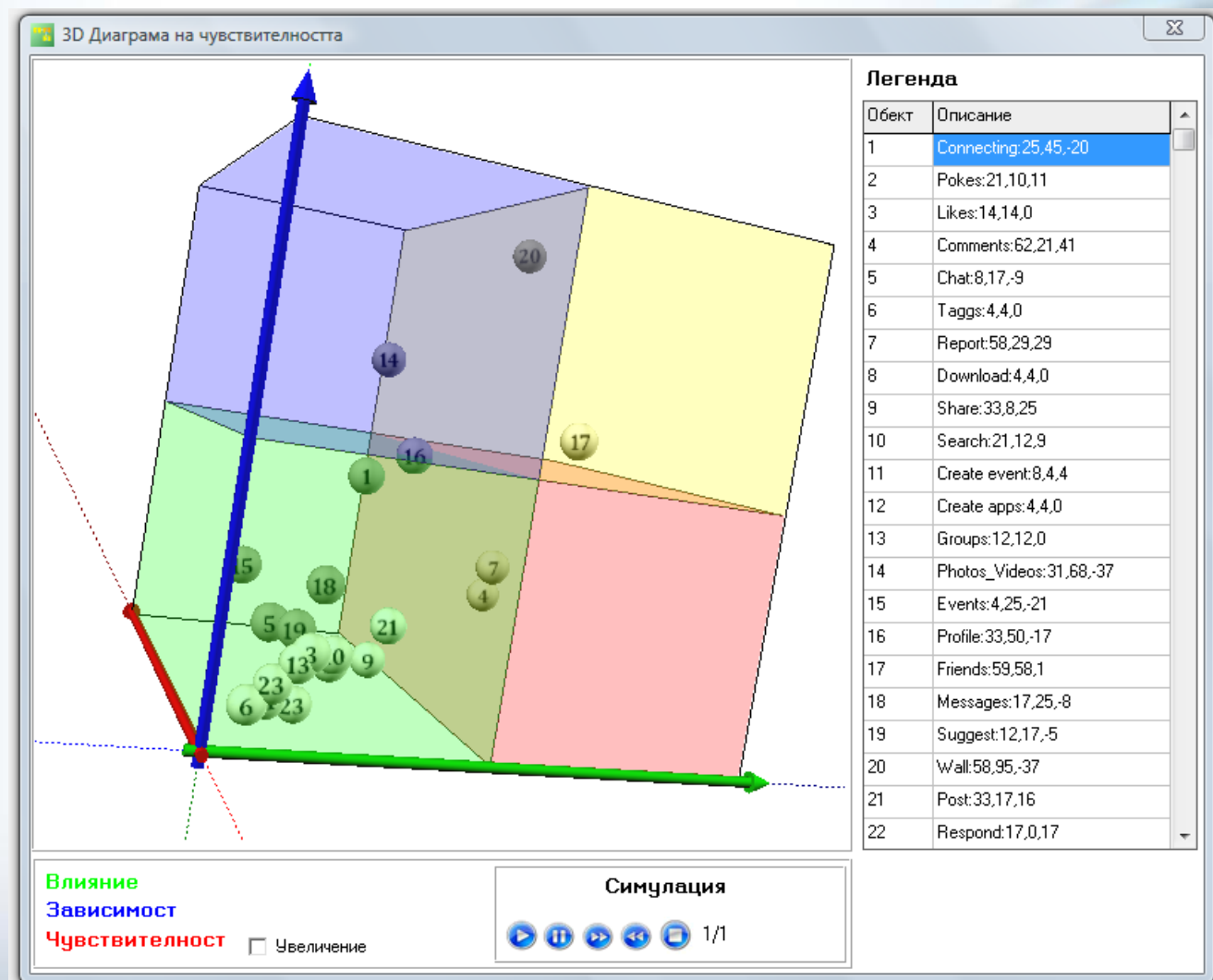
Стъпка 1: Дефиниране на обектите



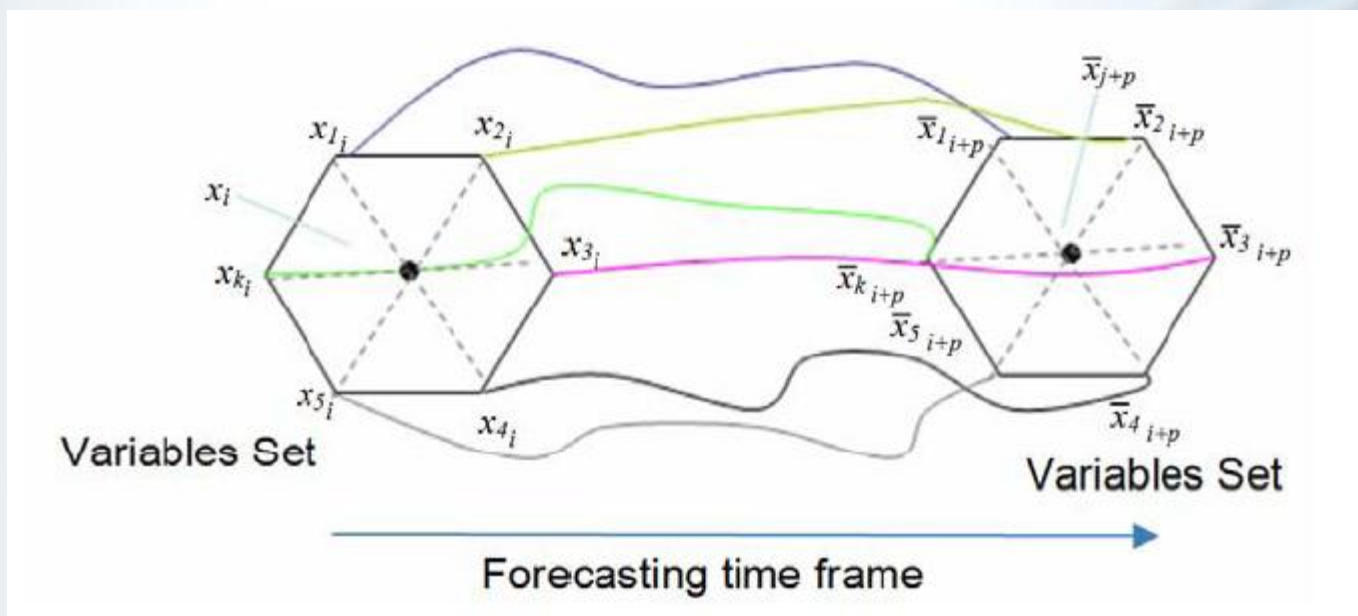
Стъпка 2: Свързване на обектите



Стъпка 3: Класифициране на обектите и анализ на чувствителността в 4D пространство



Валидиране на получените резултати



$$x_{j+p} = \sum_{i=1}^{M+1} \bar{x}_{k_{i+p}} e^{-\alpha \|x_j - x_{k_i}\|},$$

Where:

$\|\cdot\|$ is the Euclidean distance in M dimensional space;

x_{k_i} - k^{th} closest neighbour to x_i ;

$i, j > N, k + p < N, N$ is the first half of data points used for forecasting of the second one;

$\bar{x}_{k_{i+p}}$ - k^{th} closest neighbour to x_i, p steps ahead;

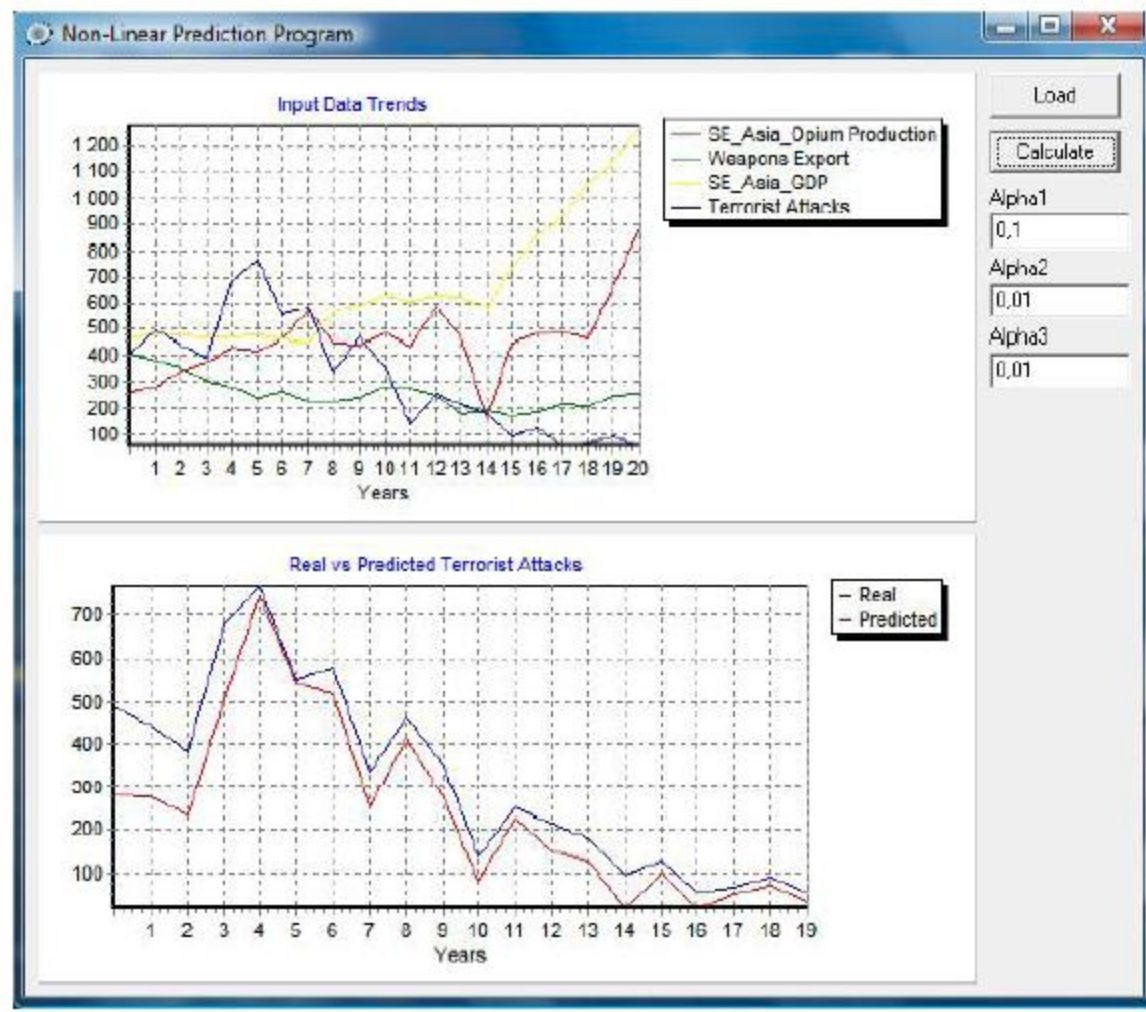
M - work space (embedding in case of single time series reconstruction) dimension;

p - number of steps ahead; α - expert-defined constants defined for the different dimensions M . The notation of space dimension M is used because the real simplex Δ^m dimension m could be initially unknown and $M < m$.

The error ε could be estimated in different ways but what was empirically evident that it is not necessary to consider ε of more than integral cubic degree of accuracy:

$$\varepsilon = |x_{i+p} - x_i| = O(h^3)$$

Софтуерна поддръжка

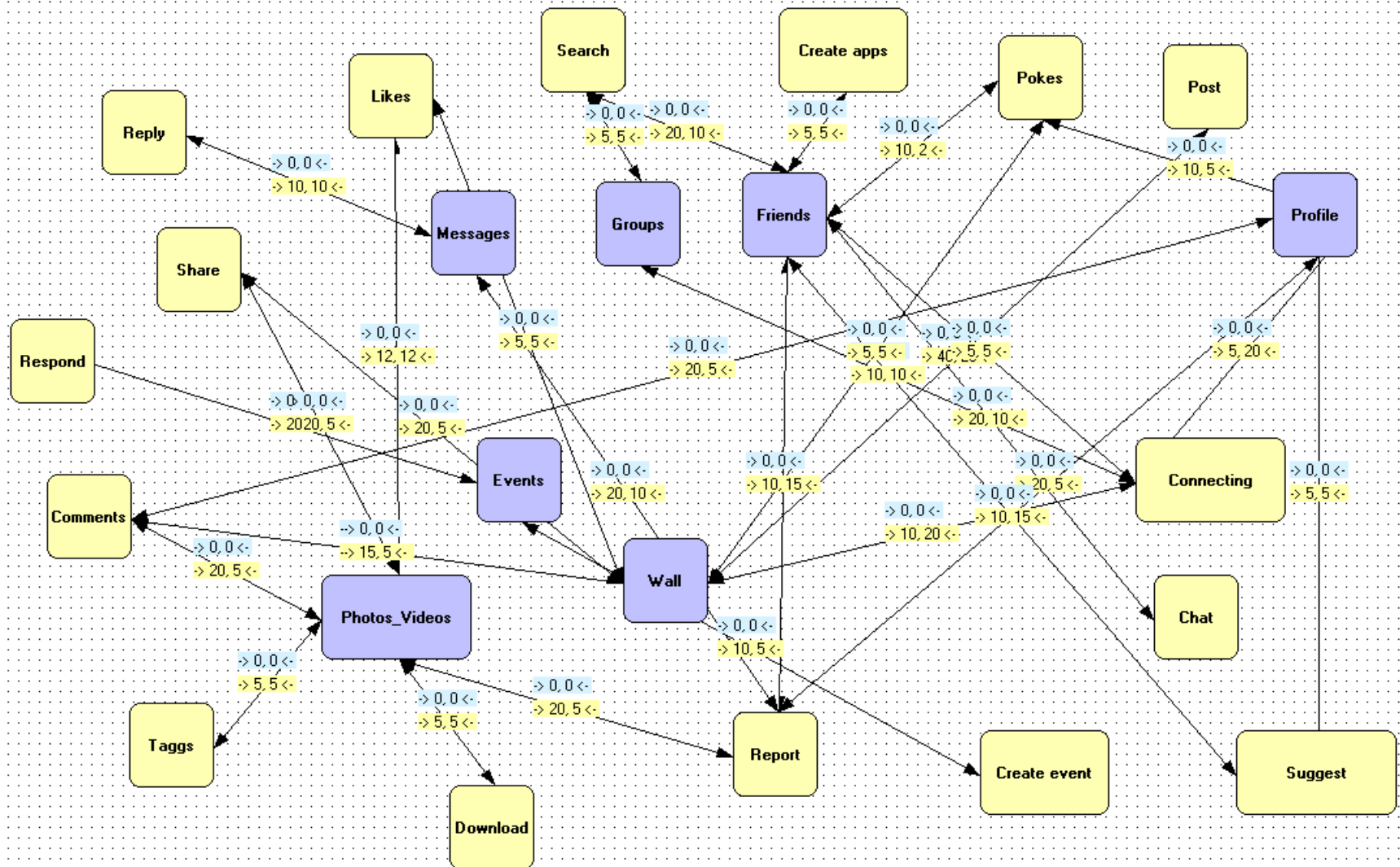


Примерни сценарии за бъдещи киберзаплахи използващи метода на сценариите

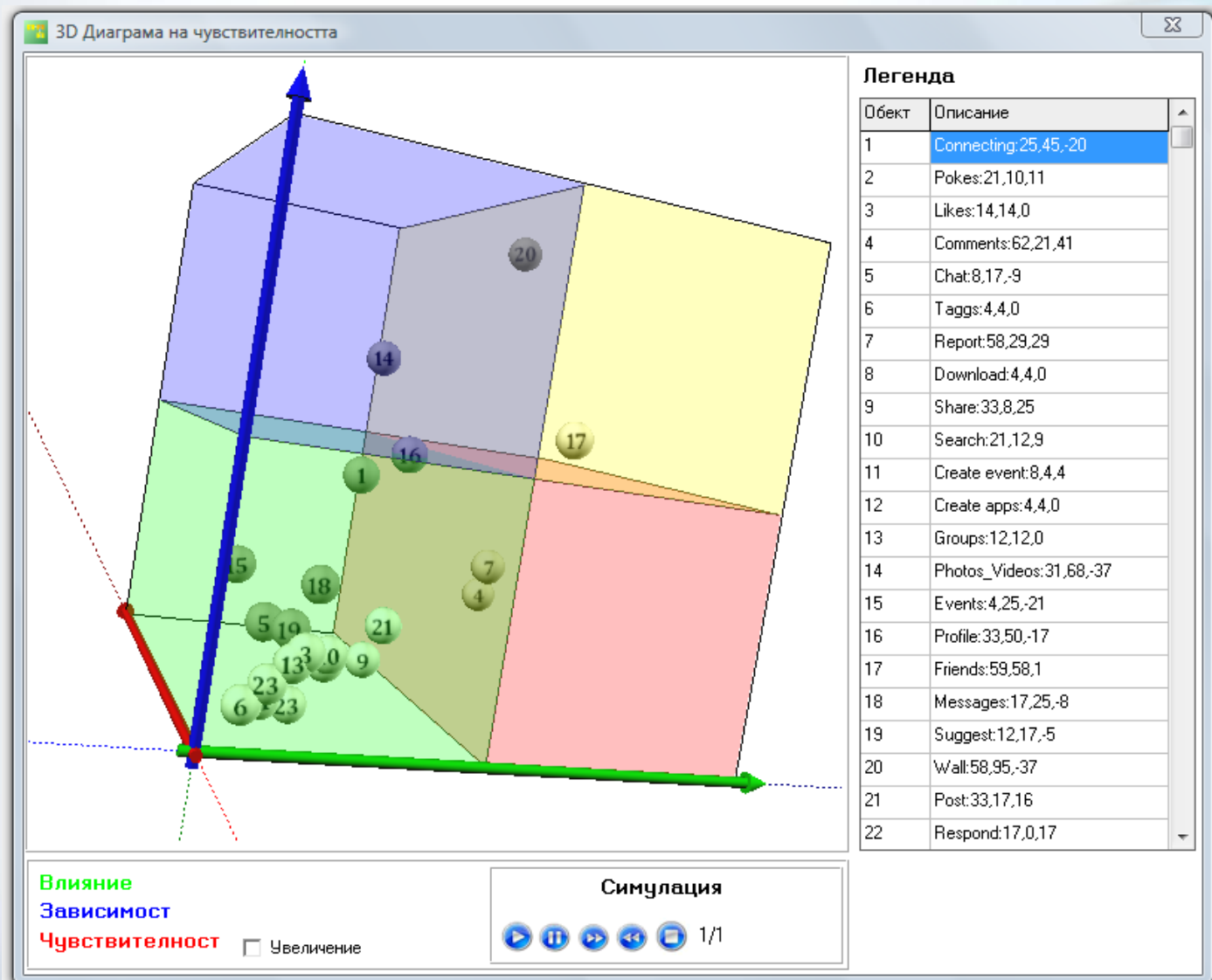
In a nutshell: Атака върху банковите сметки на частно лице използващо интелигентни мобилни устройства и персонален компютър;

The peccadillo: Атака върху интелигентни измервателни устройства с участието на организирана престъпна група.

Модел на информационните потоци в социалната мрежа Facebook



Диаграма на чувствителността



Благодаря за вниманието!

**Практическо упражнение –
Експериментално изследване
на социалната мрежа Facebook**