Нови заплахи в киберпространството

доц. д-р Златогор Минчев

Институт по информационни и комуникационни технологии-БАН

E-mail: zlatogor@bas.bg

Кръгла маса: "Състояние и проблеми на сигурността в киберпространството на България”

София, 28 Септември, 2010

Съдържание

- Заплахи в ICT инфраструктурата
- 10 сценария върху заплахите в ICT инфраструктурата
- Какви са основните заключения и общи заплахи
- Бъдещо развитие на изследванията в областта

Заплахи в ICT инфраструктурата

forward

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.

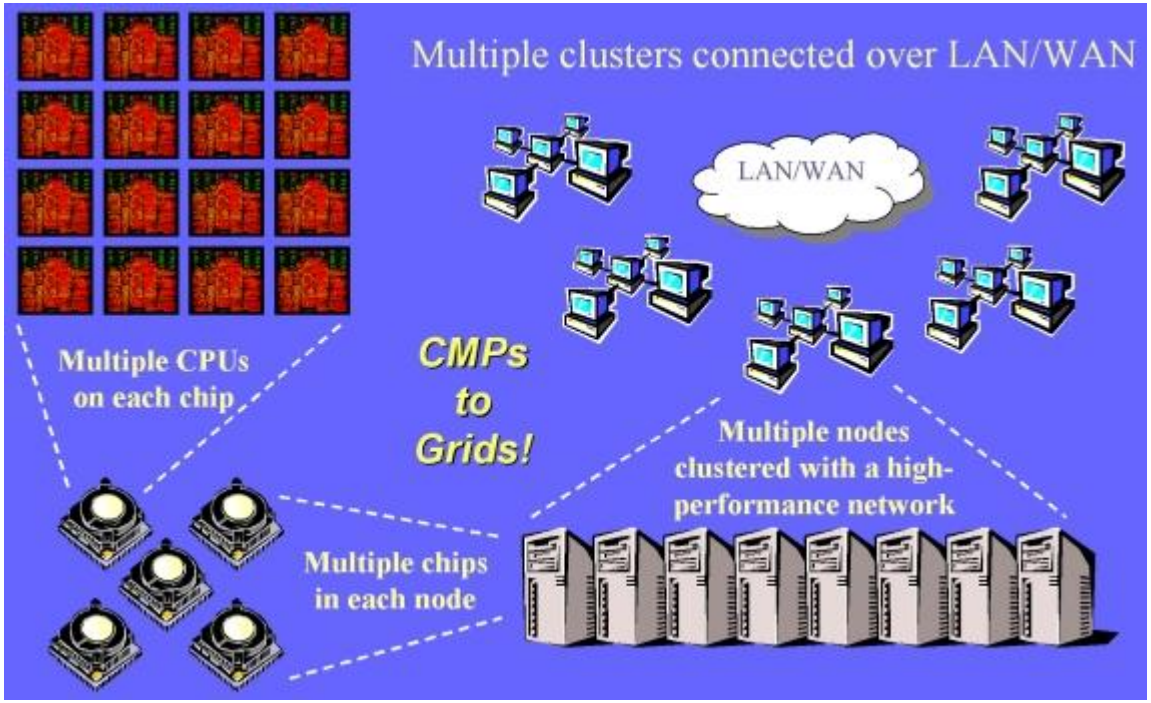
Основен резултат:

FORWARD Whitebook: Emerging ICT Threats

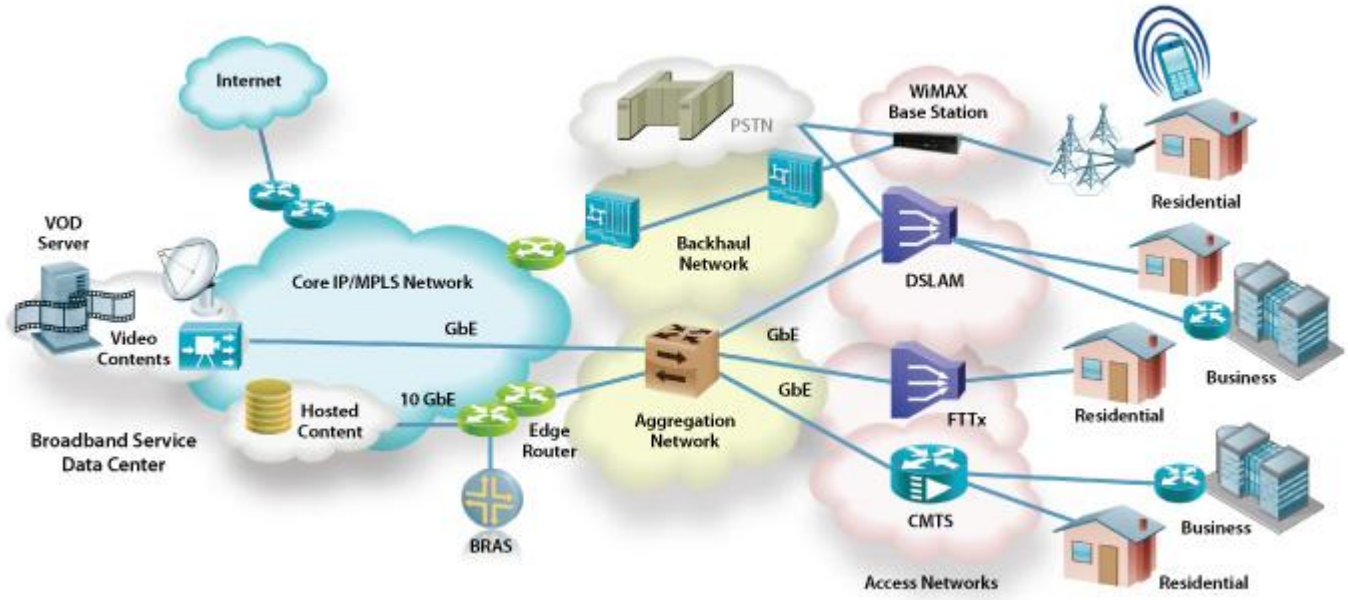
Списък на възможни бъдещи кибер заплахи

High Priority					
#	Threat Description	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

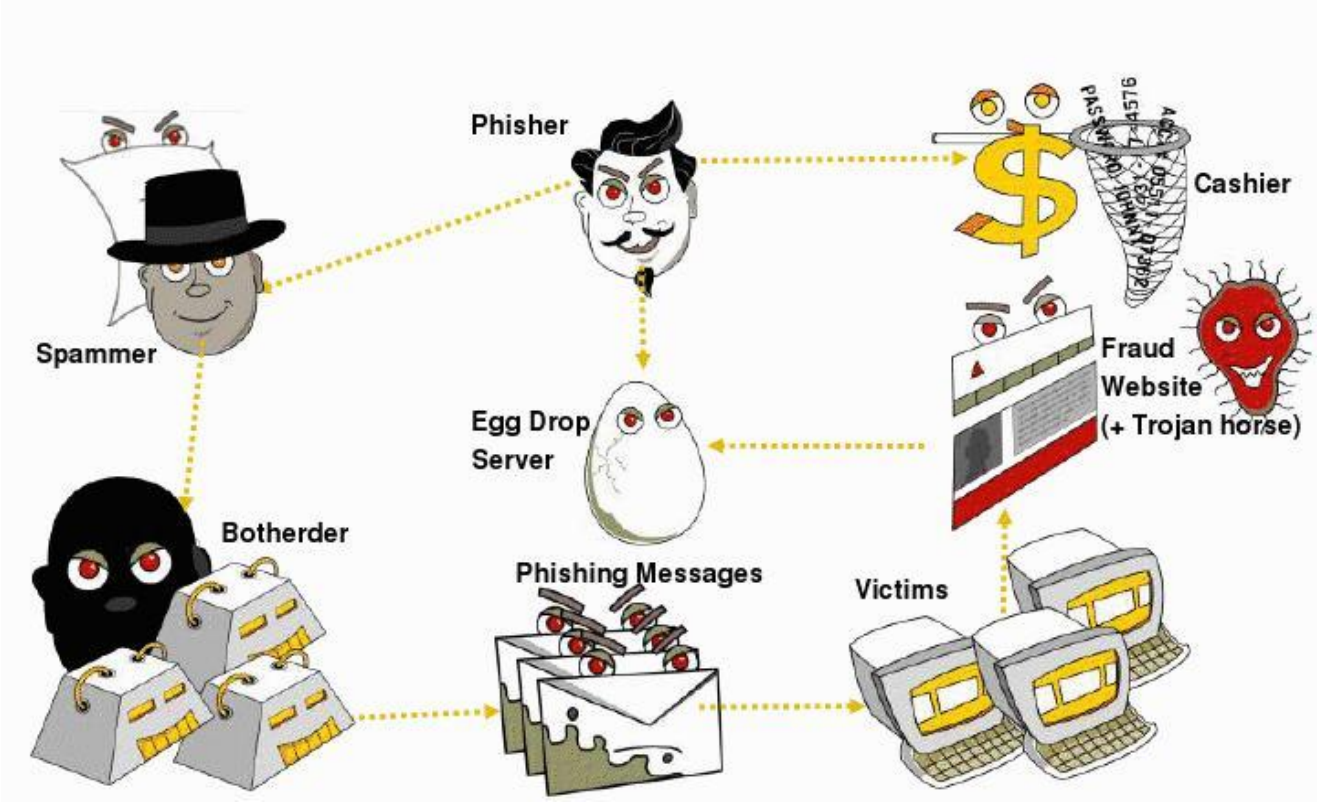
Threats due to parallelism

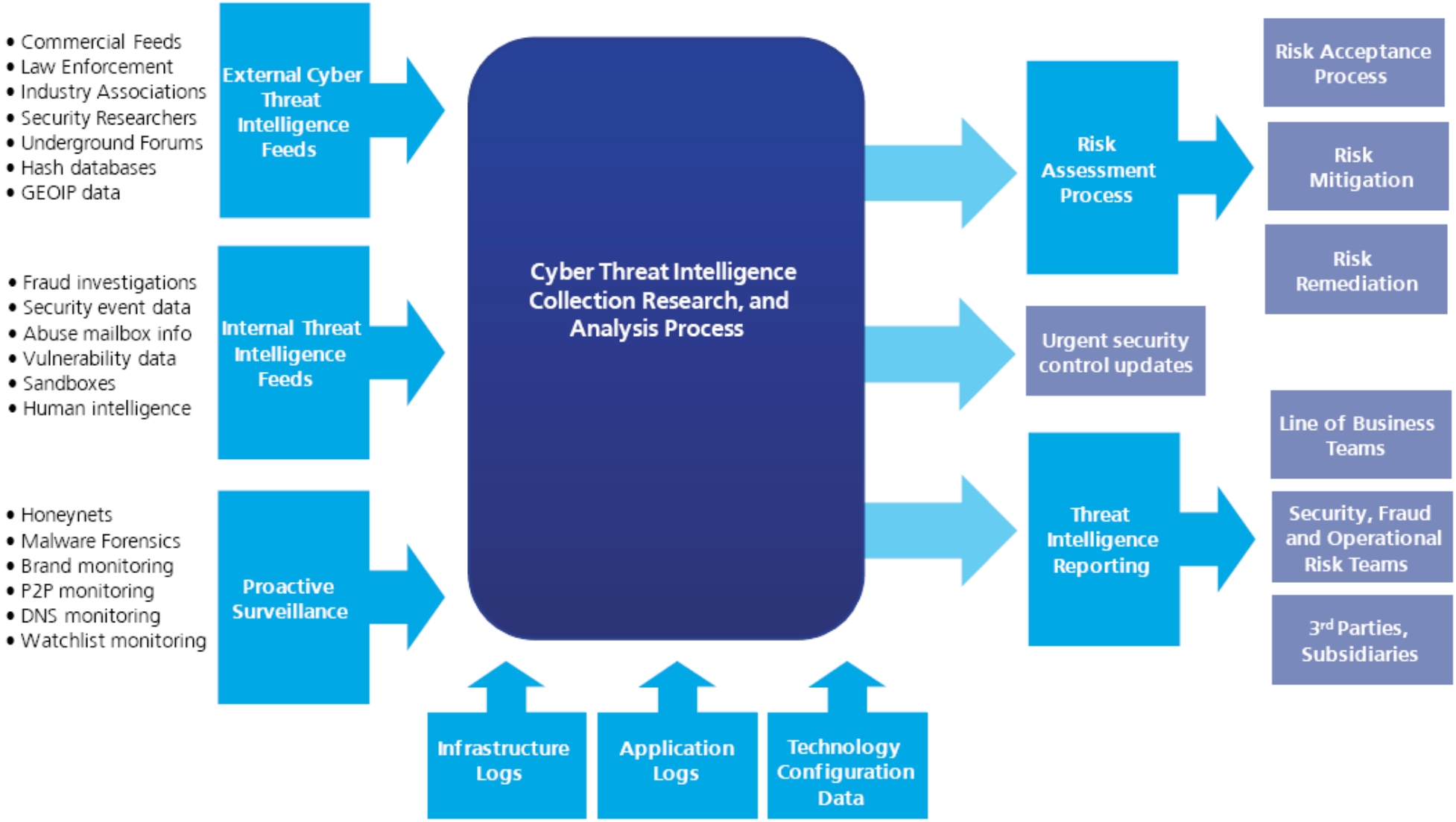


Threats due to scale



Underground economy support structures




• Commercial Feeds
• Law Enforcement
• Industry Associations
• Security Researchers
• Underground Forums
• Hash databases
• GEOIP data
External Cyber Threat Intelligence Feeds
• Fraud investigations
• Security event data
• Abuse mailbox info
• Vulnerability data
• Sandboxes
• Human intelligence
Internal Threat Intelligence Feeds
• Honeynets
• Malware Forensics
• Brand monitoring
• P2P monitoring
• DNS monitoring
• Watchlist monitoring
Proactive Surveillance
Cyber Threat Intelligence Collection Research, and Analysis Process
Infrastructure Logs
Application Logs
Technology Configuration Data
Risk Assessment Process
Urgent security control updates
Threat Intelligence Reporting
Risk Acceptance Process
Risk Mitigation
Risk Remediation
Line of Business Teams
Security, Fraud and Operational Risk Teams
3rd Parties, Subsidiaries

Mobile devices malware

Threats Related to Social Networks

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

Какви са основните заключения и общи заплахи

Мащабността на технологичното развитие!!!

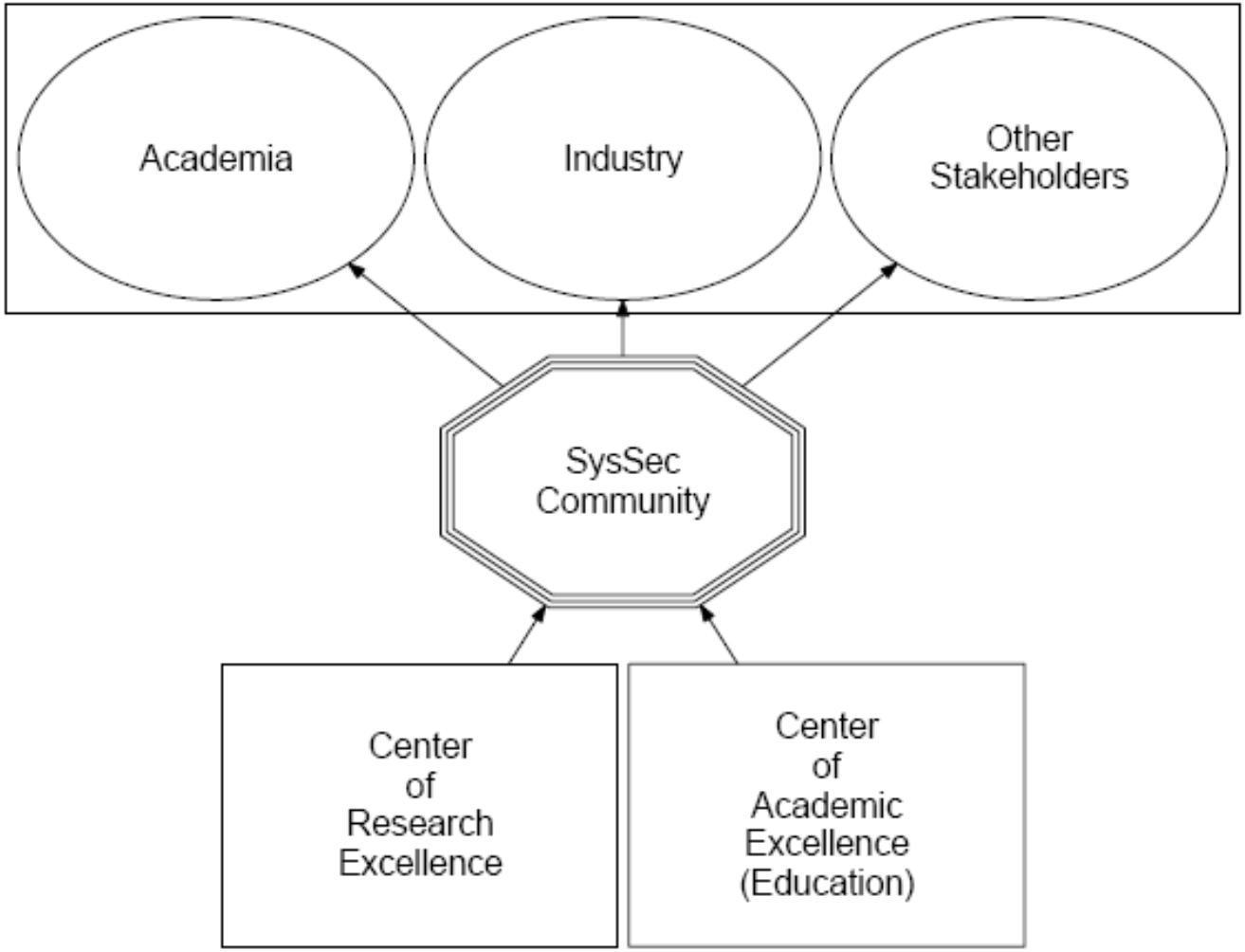
Човешкия фактор като източник на най-висока неопределеност и потенциална заплаха!!!

Бъдещо развитие на академични изследванията в областта

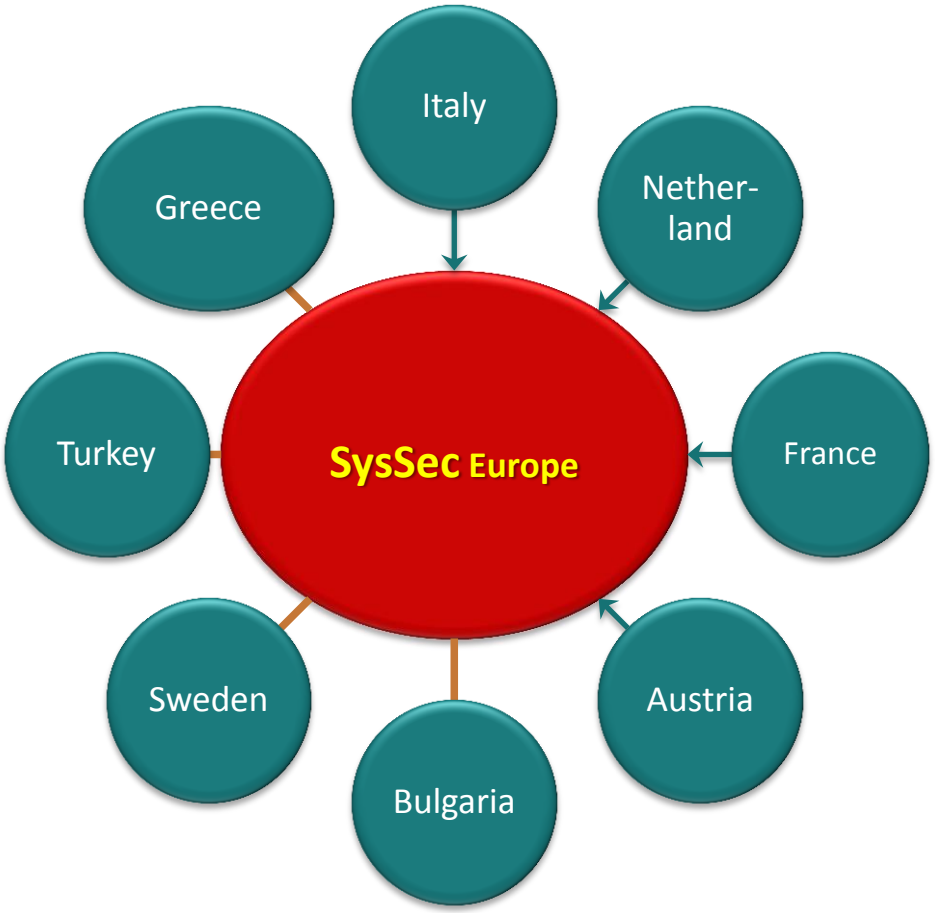
EU FP7 Project

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

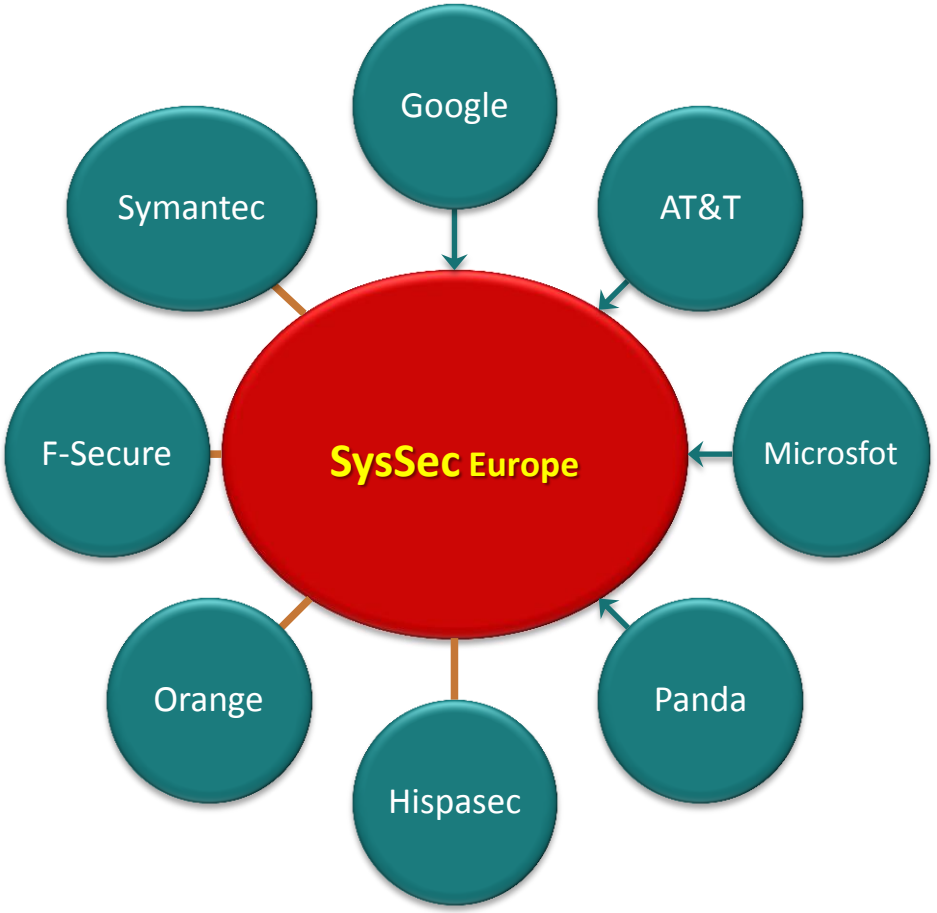
SySSec 2010 -2014


Academia
Industry
Other Stakeholders
SysSec Community
Center of Research Excellence
Center of Academic Excellence (Education)

Participating Countries



Industrial Members

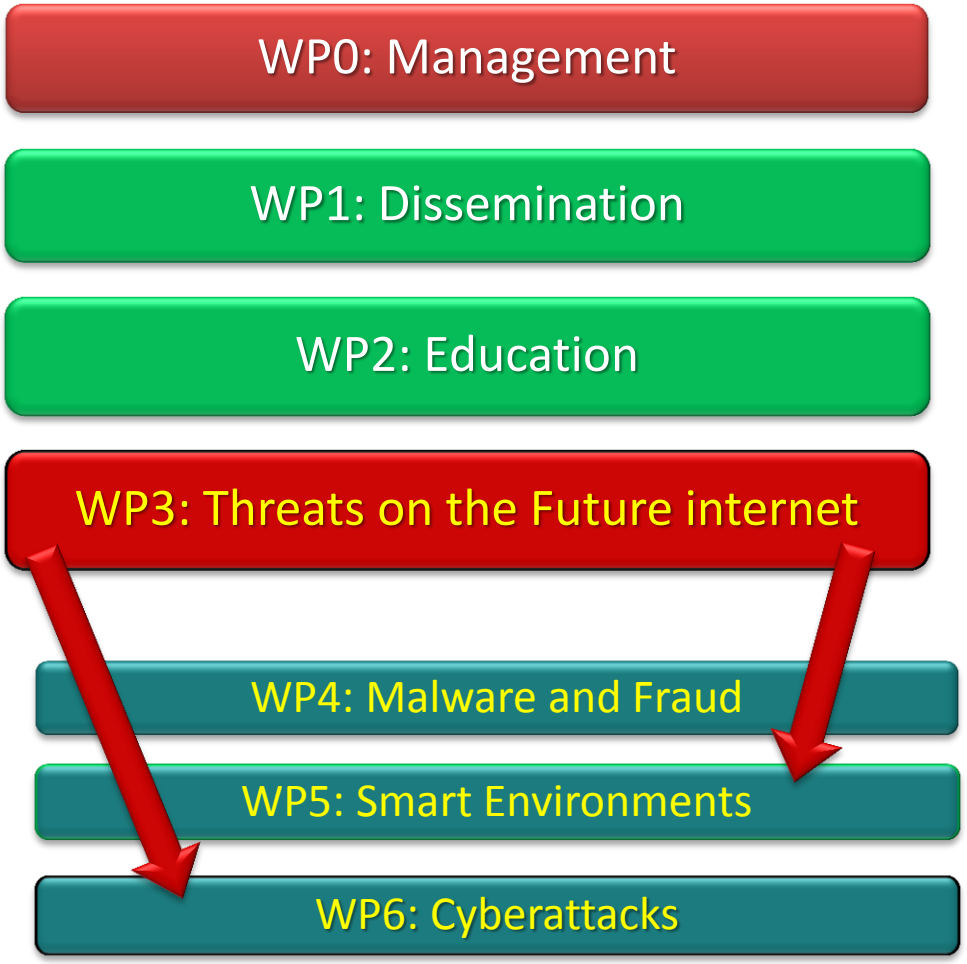


Каква е основната идея?

... Instead of *reactively* chasing after attackers,

we should start working *proactively* and think

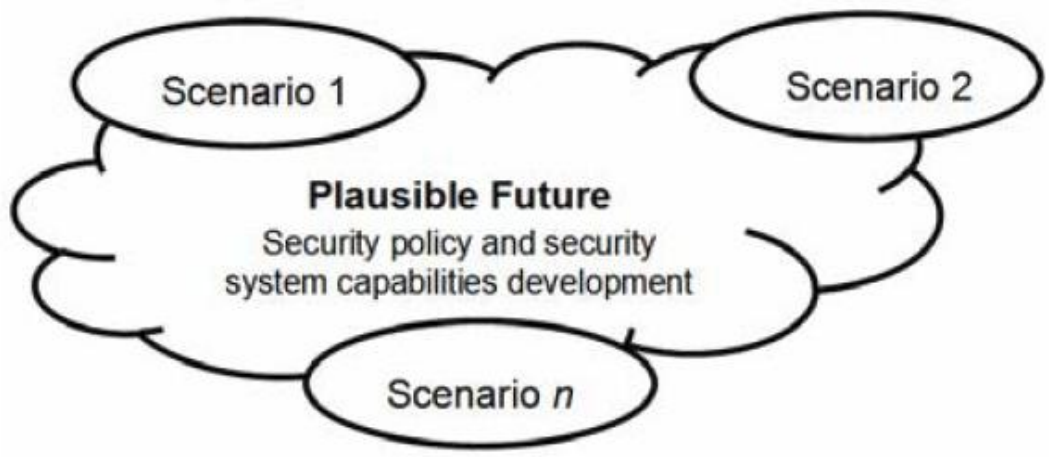
about emerging threats and vulnerabilities...



syssec

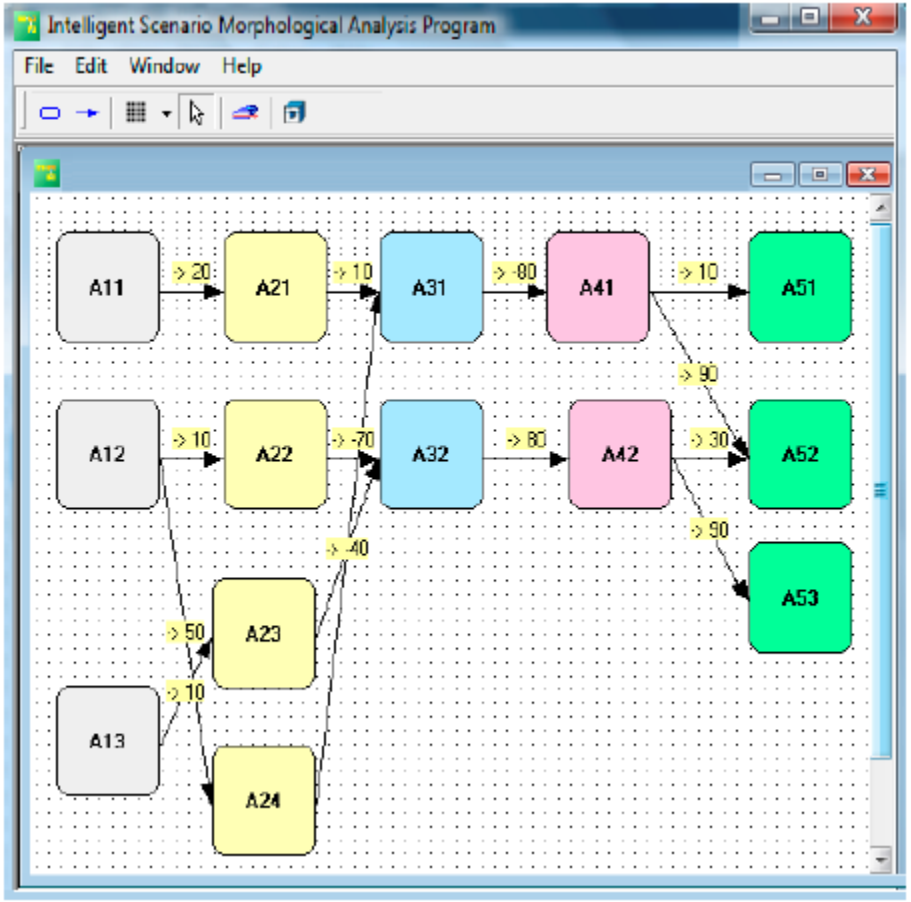
Какво планираме да направим ние?

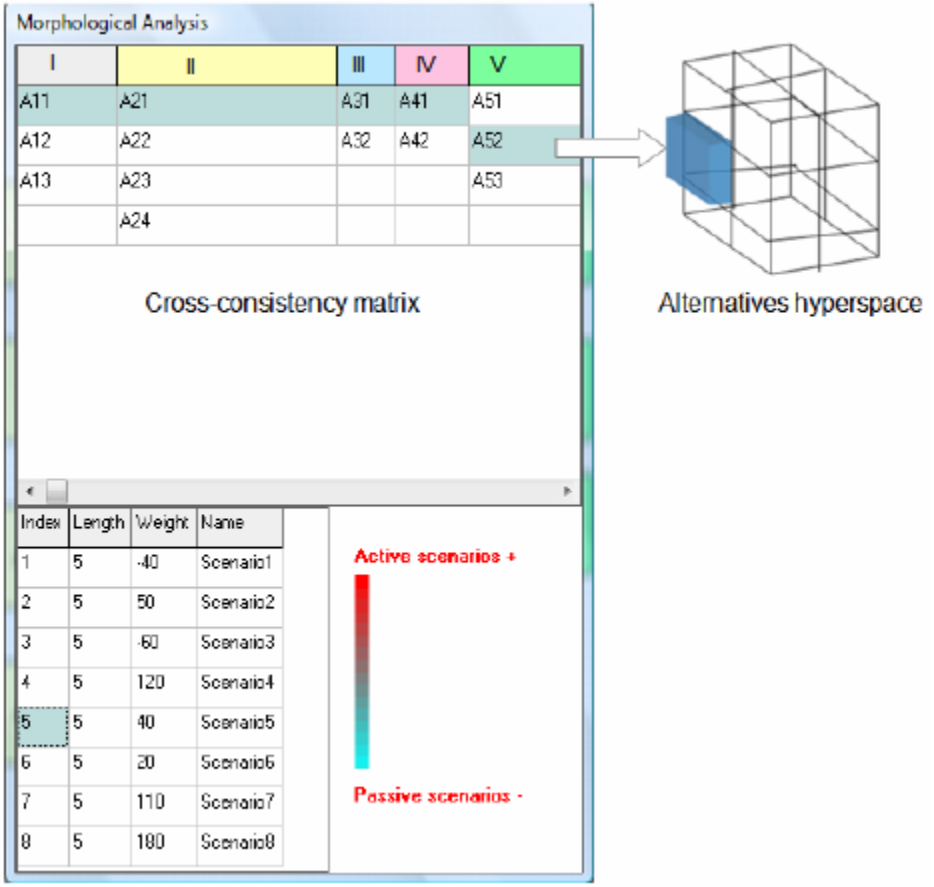
Структурен и системен анализ на бъдещите заплахи на основата на данните от проекта FORWARD и новополучени от проекта SyS Sec



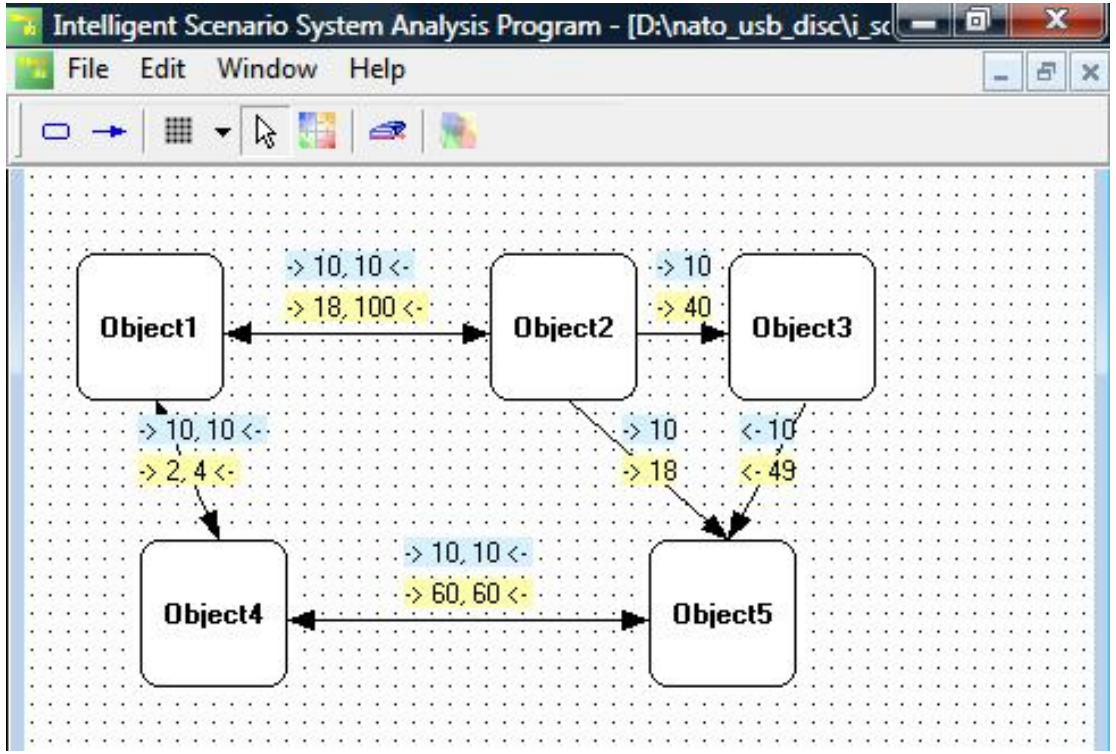
Софтуерна поддръжка

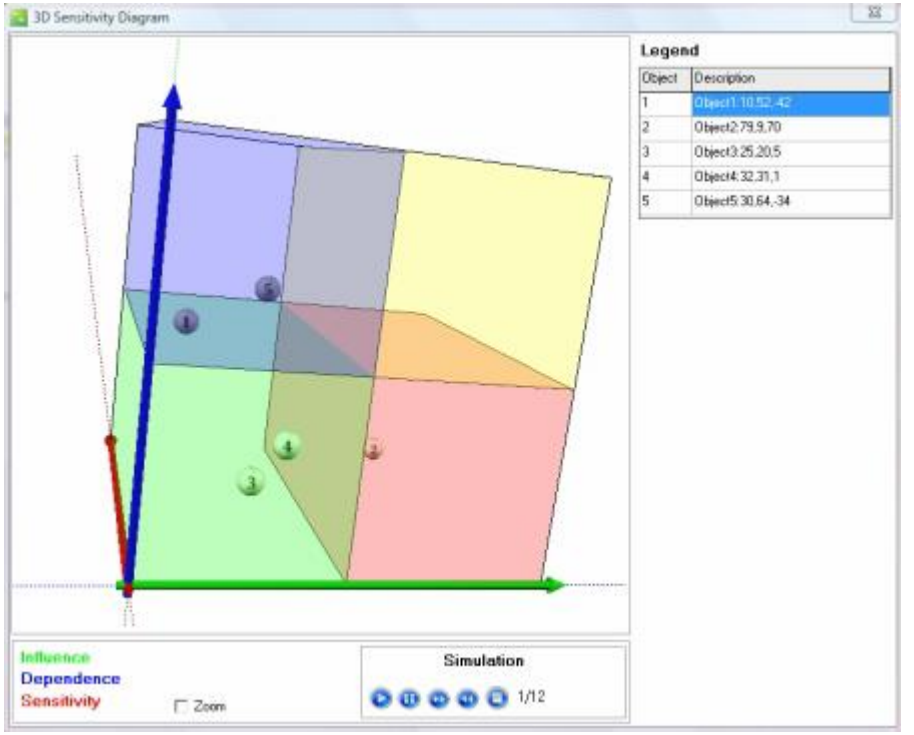
Структурен анализ





Системен анализ и анализ на чувствителността





syssec

Някои други активности в областта на киберсигурността

- European Security Research & Innovation Forum – ESRIF, 2009
- NATO ACT Cyber Defence Framework, 2010
- NC3A Multinational Cyber Defence Program, 2010

Благодаря за вниманието!