New Cyber Security Challenges

Assoc. Prof. Zlatogor Minchev, PhD

Institute of ICT- Bulgarian Academy of Sciences

E-mail: *zlatogor@bas.bg*

AFCEA
VARNA

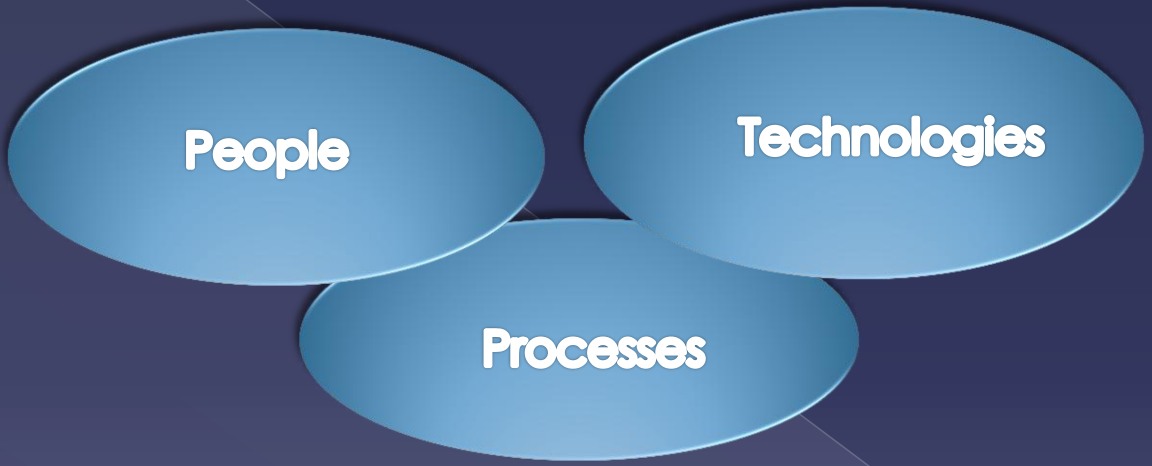
10th Anniversary

International Conference
"C4ISR in South-Eastern Europe – Problems and Solutions"

OUTLINE

- What to address today in cyber security?
- ICT infrastructure threats
- How to continue?
- What is missing?
- Other activities related to cyber security

What to address today in cyber security?



Building Capabilities in all these !!!

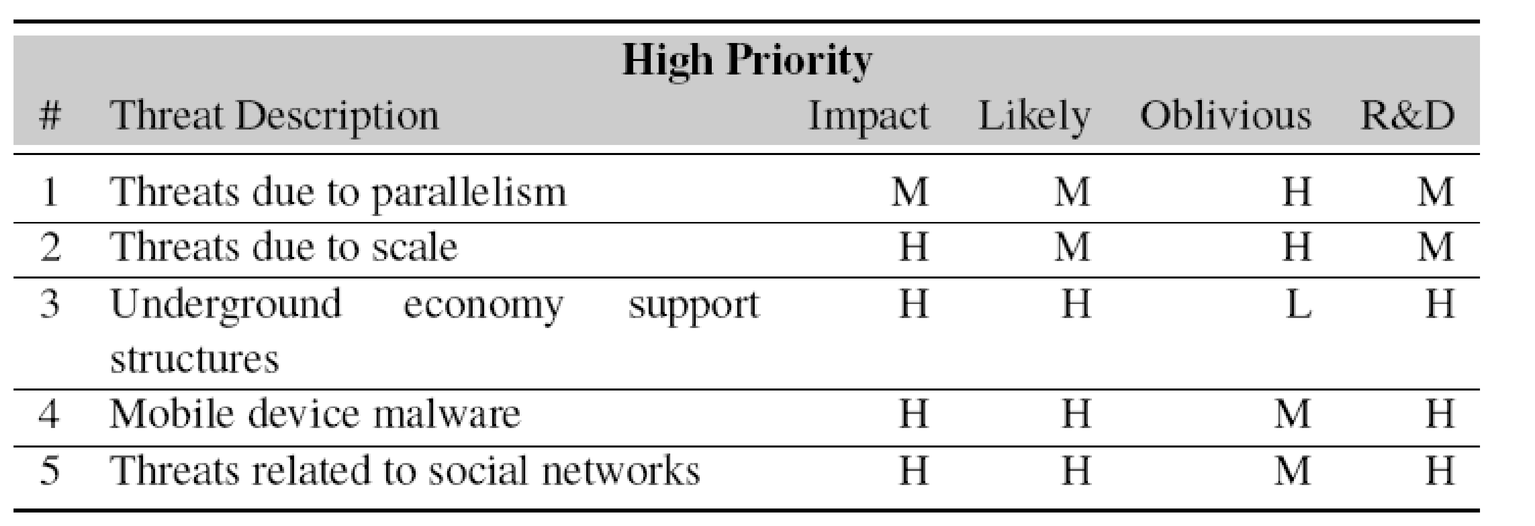
ICT INFRASTRUCTURE THREATS

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.

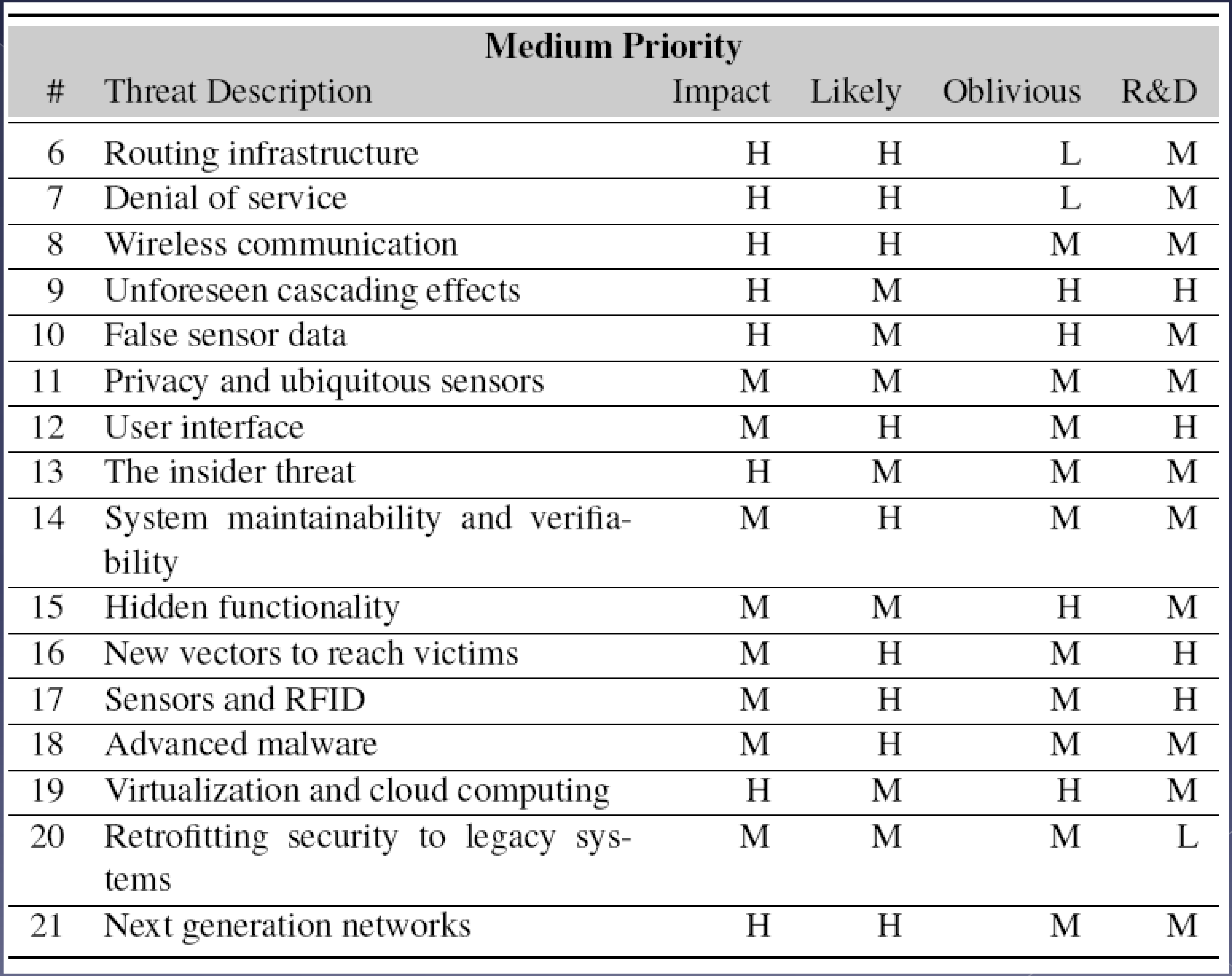
Basic Result:

FORWARD WHITEBOOK: "EMERGING ICT THREATS"

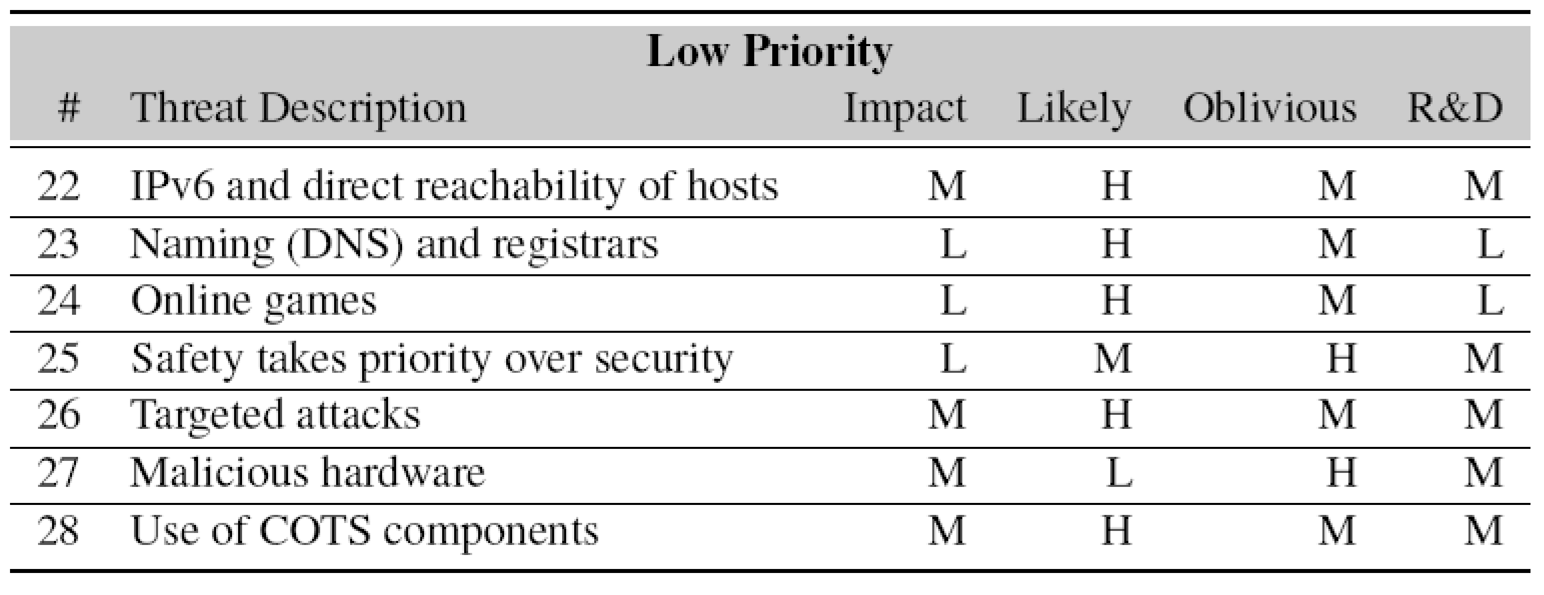
POSSIBLE CYBER THREATS



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



	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

How to continue?

To work together in a network!

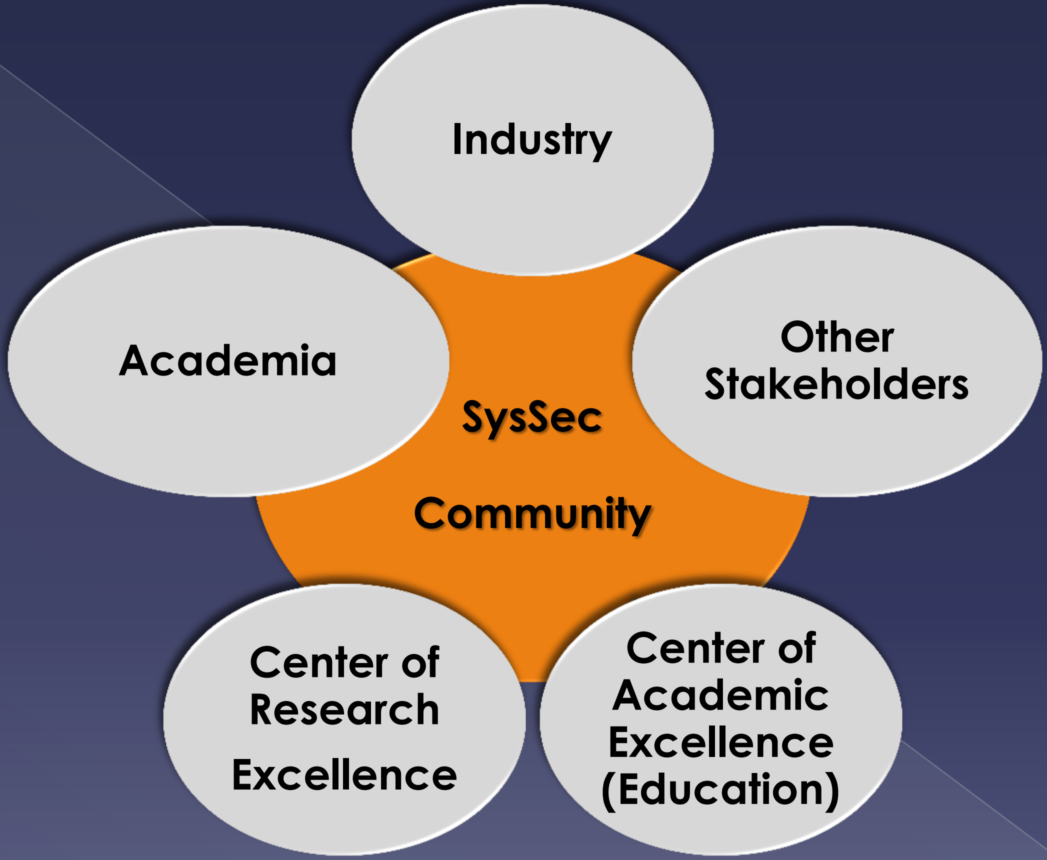
A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World, EU FP7

SySSec 2010 -2014

syssec

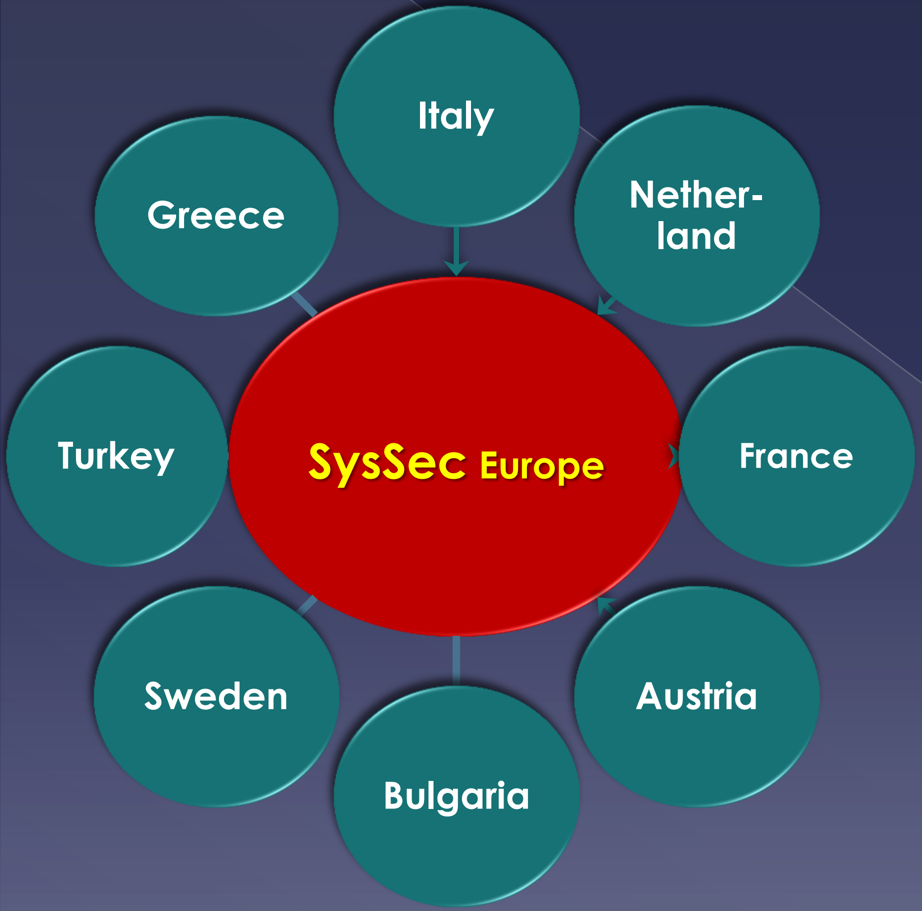
... Instead of reactively chasing after attackers, we should start working proactively and think about emerging threats and vulnerabilities...

The Consortia


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

syssec

Participating Countries & Industry



SysSec Europe

Italy

Greece

Nether-land

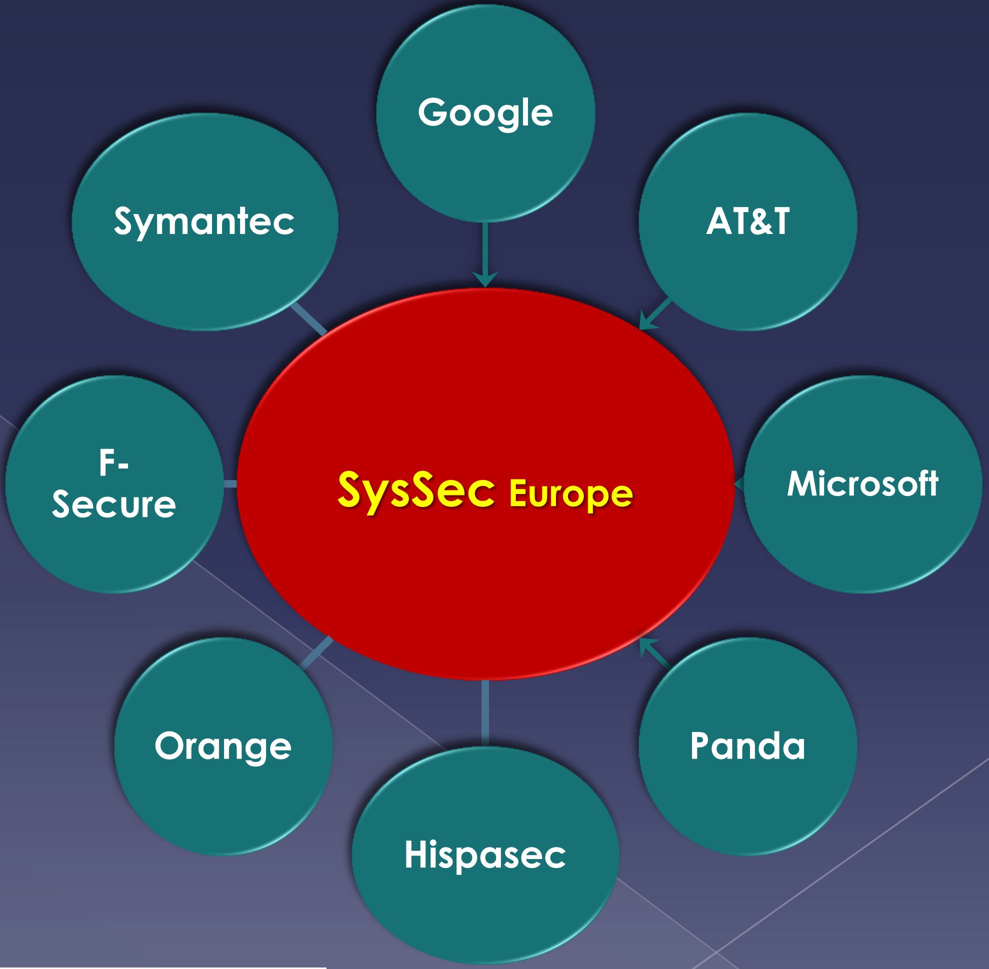
Turkey

France

Sweden

Bulgaria

Austria



SysSec Europe

Google

Symantec

AT&T

F-Secure

Microsoft

Orange

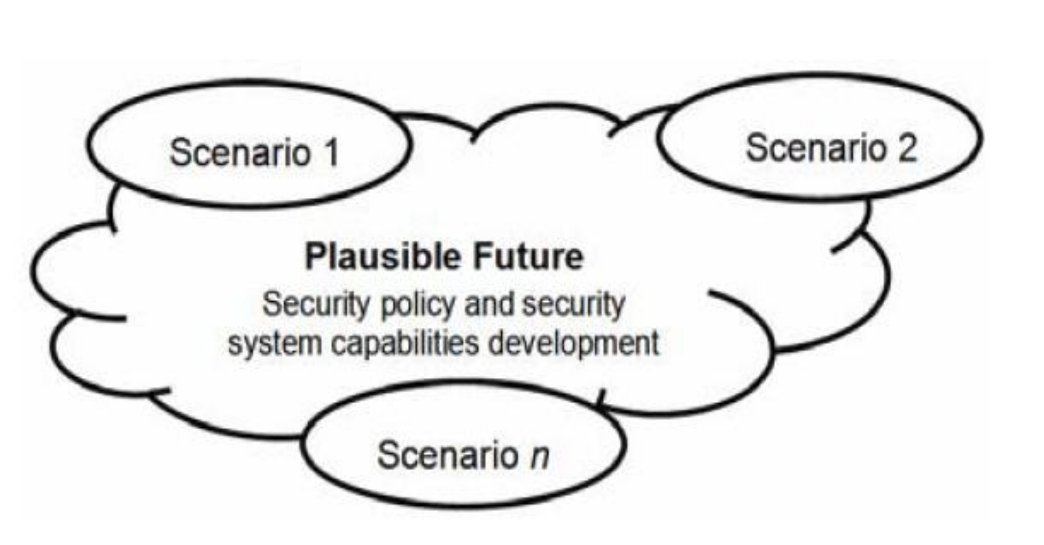
Hispasec

Panda

syssec

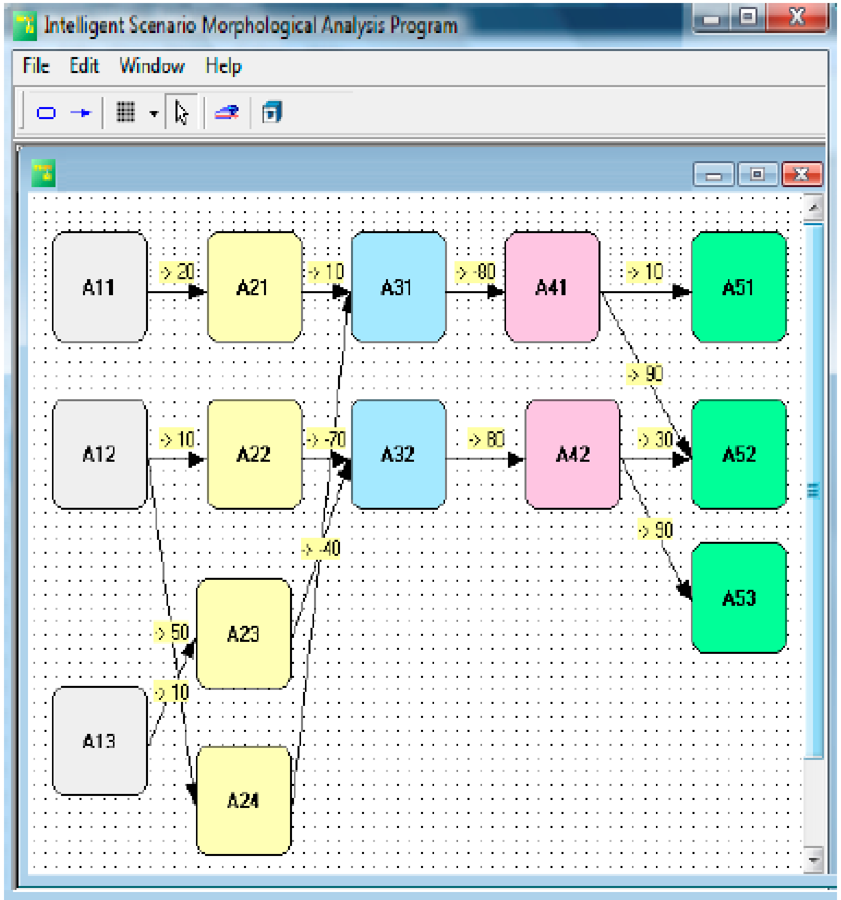
What is missing?

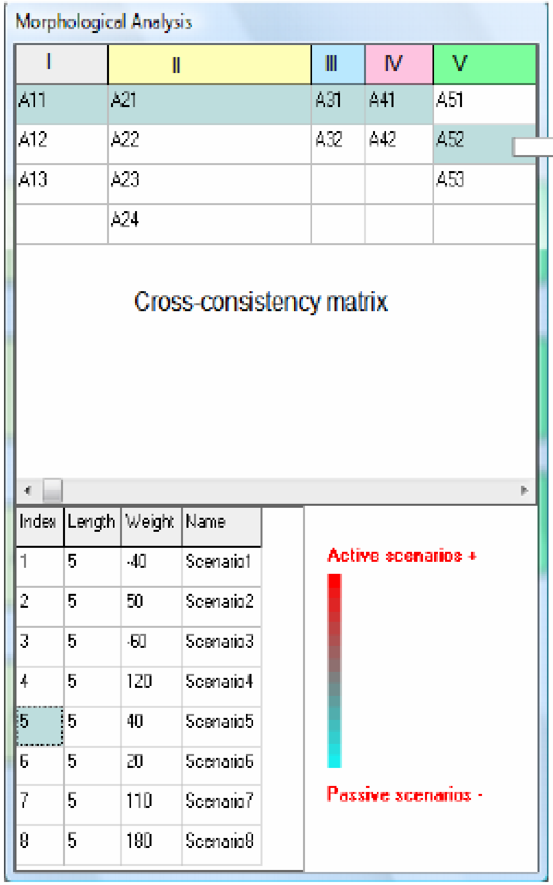
Morphological & system analysis of the data for determining the future cyber threats in a certain selected context


Scenario 1
Scenario 2
Plausible Future
Security policy and security system capabilities development
Scenario *n*

syssec

Morphological Analysis

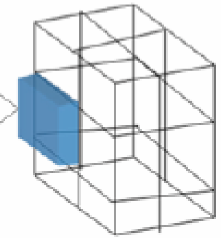




I	II	III	IV	V
A11	A21	A31	A41	A51
A12	A22	A32	A42	A52
A13	A23			A53
	A24			

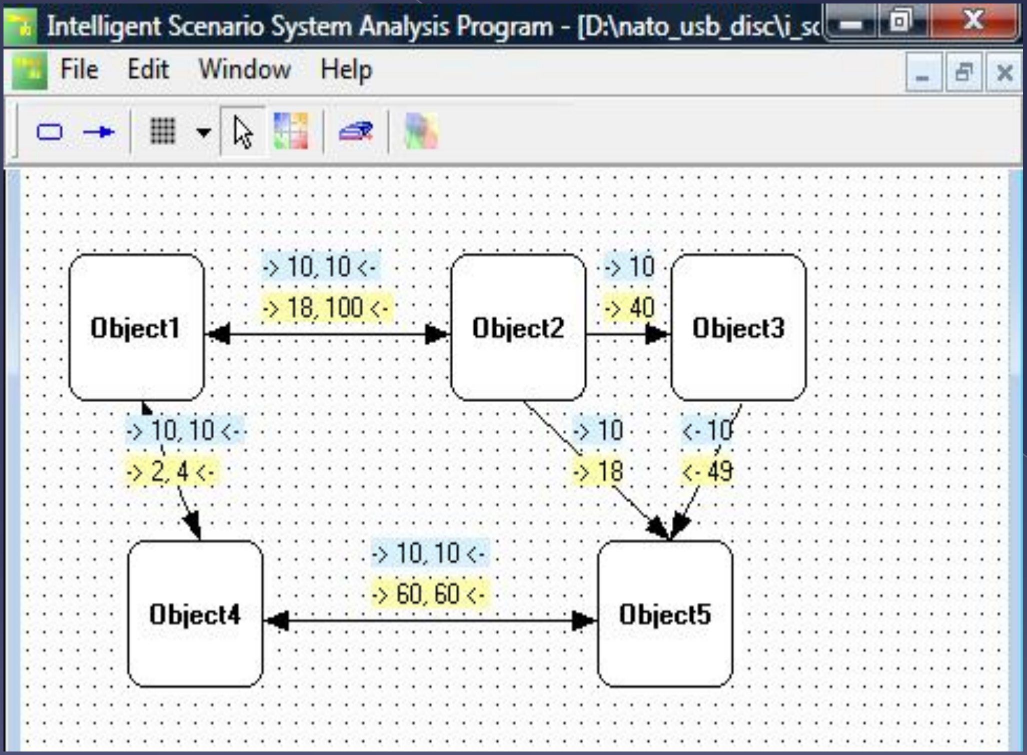
Cross-consistency matrix

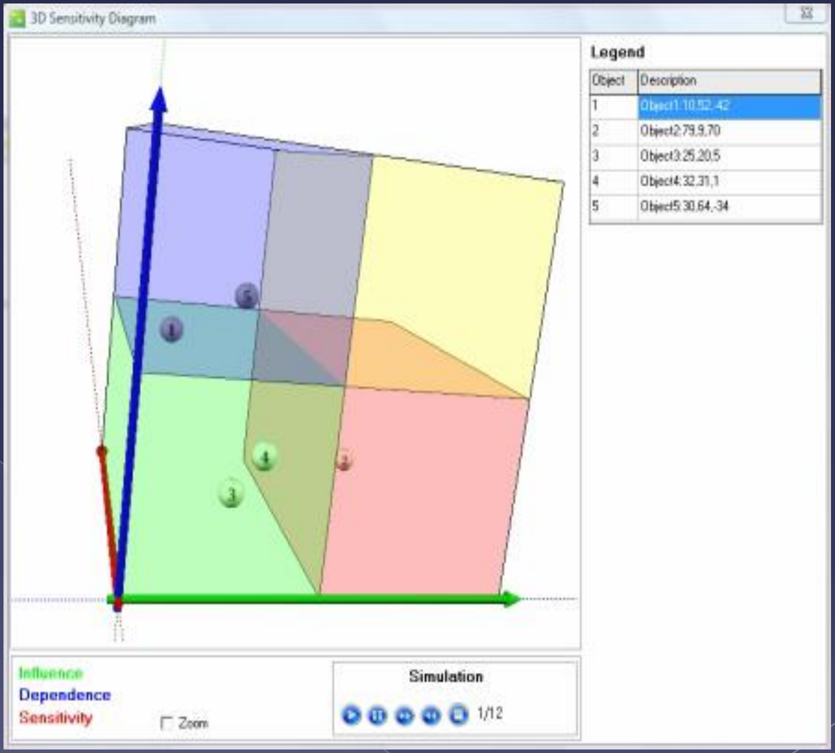
Index	Length	Weight	Name
1	5	-40	Scenario1
2	5	50	Scenario2
3	5	-60	Scenario3
4	5	120	Scenario4
5	5	40	Scenario5
6	5	20	Scenario6
7	5	110	Scenario7
8	5	180	Scenario8



Alternatives hyperspace

System Analysis


Intelligent Scenario System Analysis Program - [D:\nato_usb_disc\i_sc


3D Sensitivity Diagram

Legend

Object	Description
1	Object1:10,52,42
2	Object2:79,9,70
3	Object3:25,20,5
4	Object4:32,31,1
5	Object5:30,64,-34

syssec

OTHER RECENT ACTIVITIES RELATED TO CYBER SECURITY

- European Security Research & Innovation Forum – ESRIF – EC FP7, 2007 - 2009
- Worldwide Observatory of Malicious Behaviors and Attack Threats – WOMBAT – EC FP7, 2008 - 2010
- NATO ACT Cyber Defence Framework, 2010
- NC3A Multinational Cyber Defence Program, 2010
- NATO Emerging Security Challenges Division, August, 2010

THANK YOU FOR THE ATTENTION!