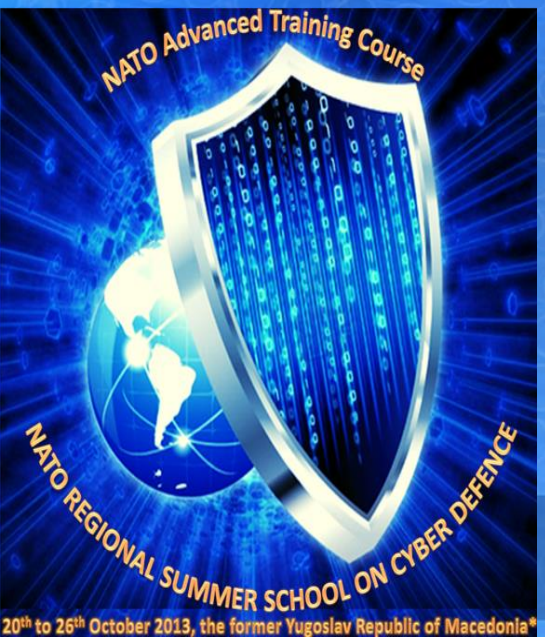
NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

Cyber Risks & Threats. State of the art & future trends

A Comprehensive Methodological Overview with Examples



Assoc. Prof. Dr. Zlatogor Minchev
IICT

Contents

- Nowadays Cyberworld
- Cyberthreats & Risks Identification
- Context Generation
- Extracted knowledge analysis
- Psychophysiological Validation
- Some Implementation Examples
- Discussion

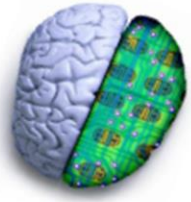
NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

NOWADAYS CYBERWORLD













NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Technological Challenges

2000

Web 1.0

Web 2.0

Web 5.0

Web 3.0

2050

Web 4.0

NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Cyberthreats & Risks Identification

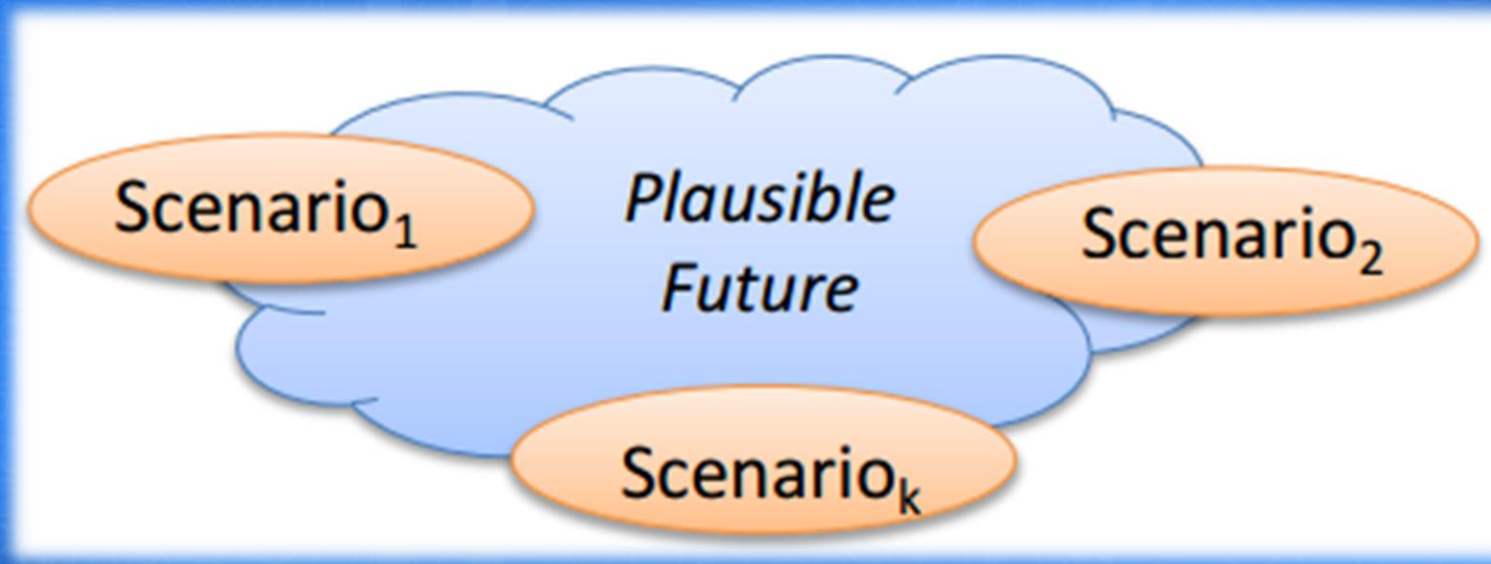
Human-Machine Interaction

Methodological Analysis Framework

- ❑ Context Generation
- ❑ Analysis
- ❑ Validation

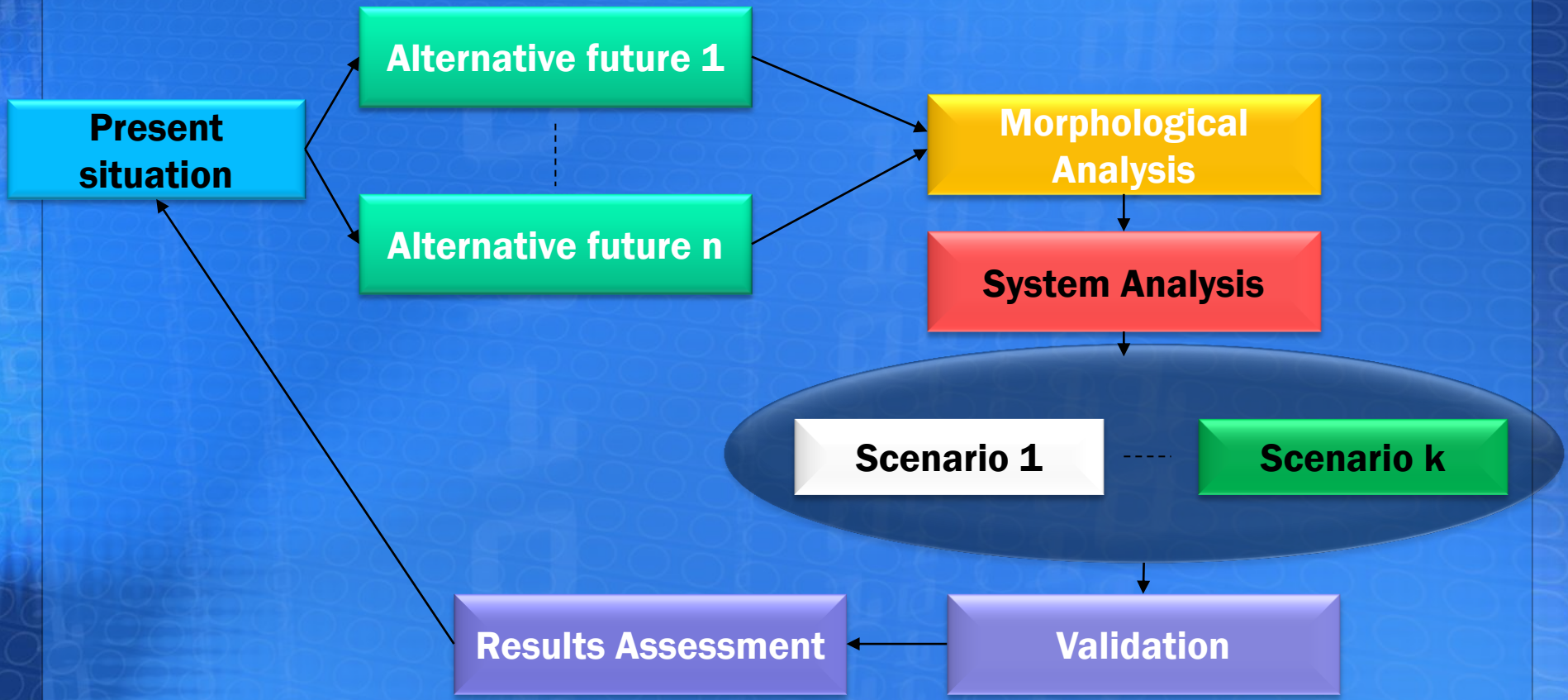
NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

Context Generation



This activity is supported by: The NATO Science for Peace and Security Programme

The Scenario Generation Process



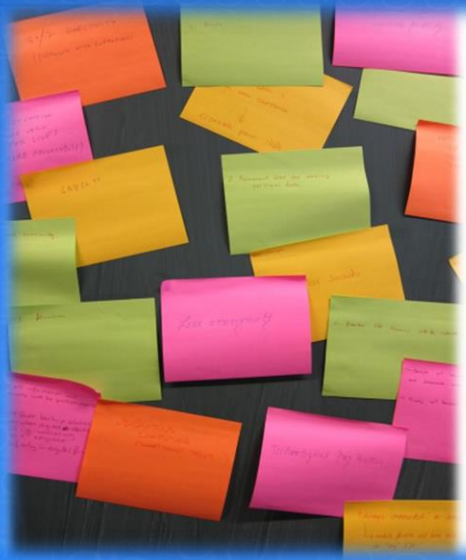
NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

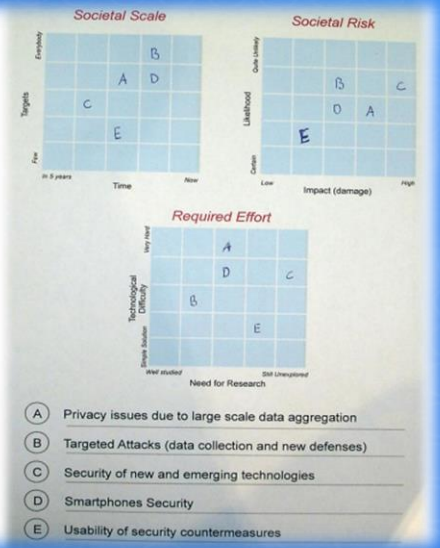
EXPERTS' KNOWLEDGE EXTRACTION

- BRAINSTORMING
- DISCUSSIONS
- DELPHI METHOD BASED ON QUESTIONNAIRES

NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

SOME DATA AGGREGATION EXAMPLES





Questionnaire

Smart Homes User Based Cyber Threats Evaluation
* Required

What kind of smart devices you are currently using in your everyday life? *

- [ ] Smart Phone
- [ ] Tablet
- [ ] Laptop/Ultrabook
- [ ] Smart TV
- [ ] Companion Robot
- [ ] Automated everyday life systems
- [ ] Gamming consoles
- [ ] Other:

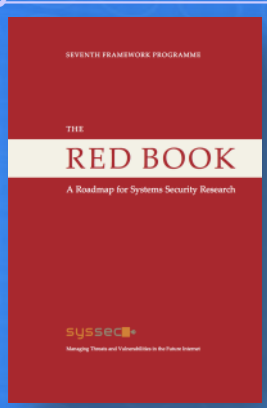
What usually do you do with smart devices in your everyday life?

- [ ] Entertainment
- [ ] Everyday work support
- [ ] Household support
- [ ] Communications/Contacting

Cyberthreats 2012

Threat source \ Dimension	Threats weight	R&D Role	Time & Users
Privacy information aspects in system security			
Targeted attacks			
Emerging Technologies			
Mobile devices security			
Usable security			

Cyberthreats 2013



NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

Key Problems

- Experts selection
- Proper understanding
- Noise reduction
- Human subjectiveness
- Software support necessity
- Validation Difficulties

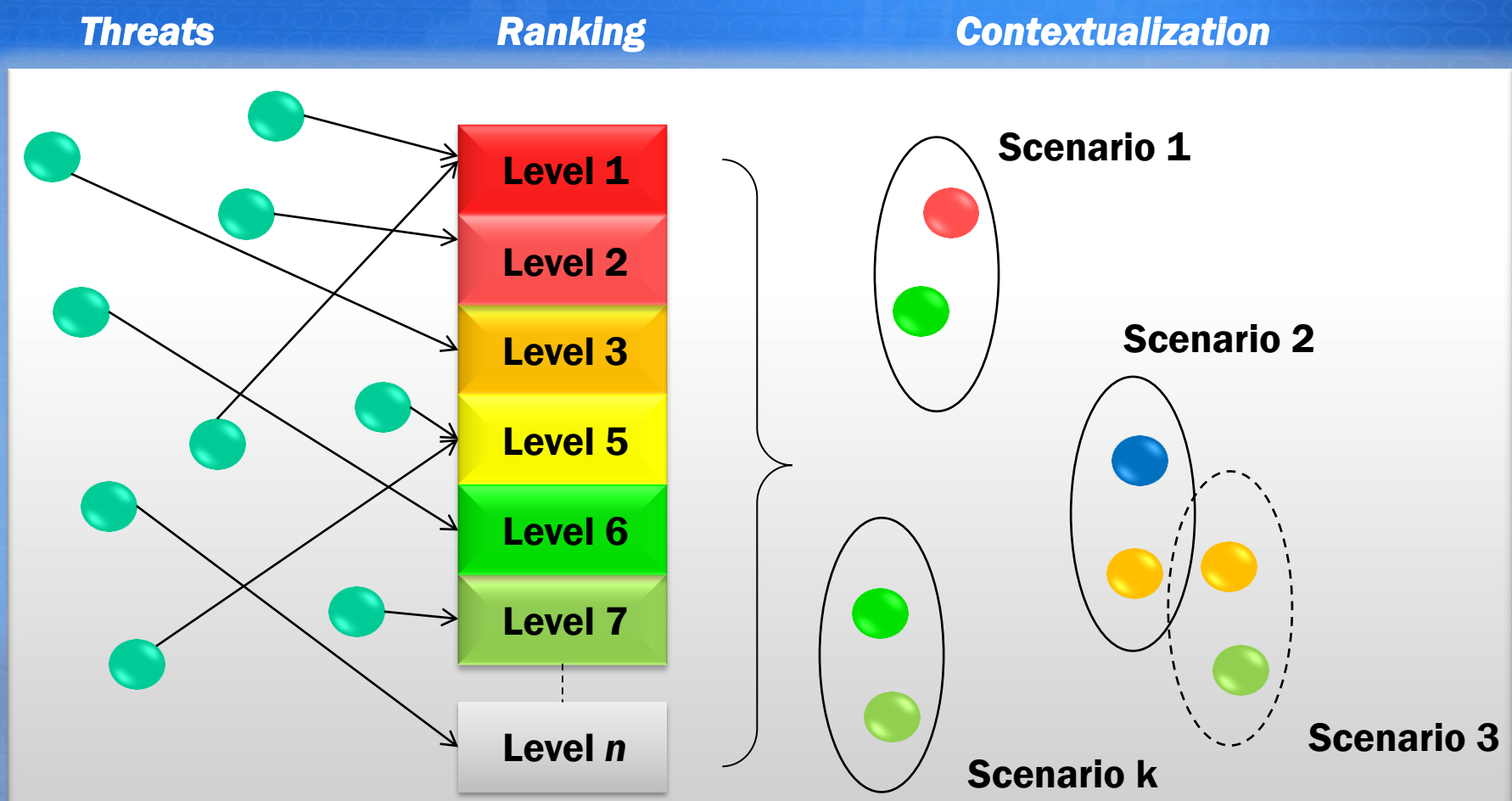
NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

Threats Identification & Contextualization

- Proper threats identification is context dependable;
- Ranking is inevitable;
- Overlapping is difficult to surmount.

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

Ranking & Contextualization



NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Extracted knowledge analysis

Techniques:

Morphological analysis;

System analysis;

Working environment:

MS Office/OpenOffice;

Intelligent Scenario Computer Interface Program (I-SCIP).

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

MORPHOLOGICAL ANALYSIS

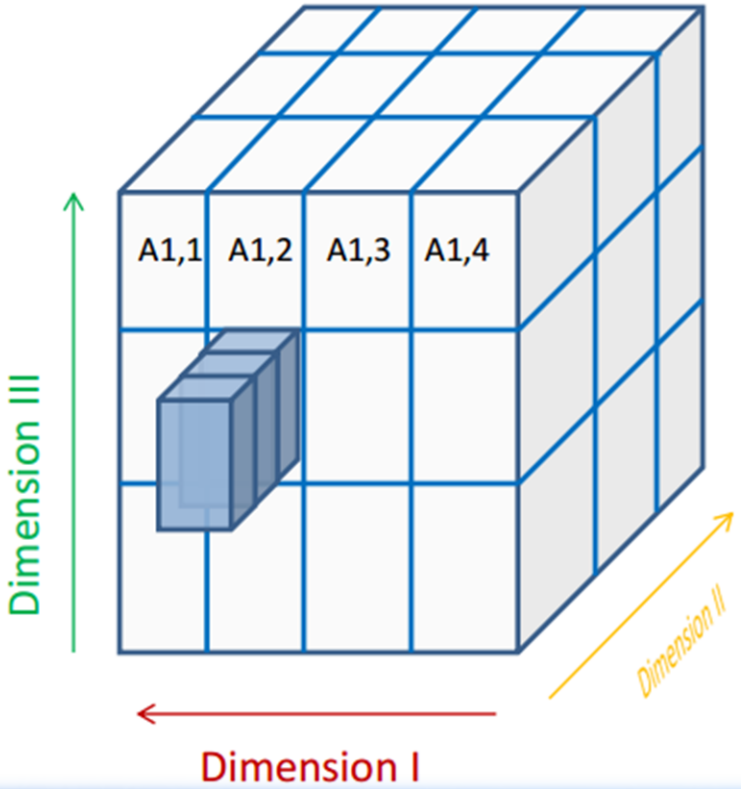
- COMPLETE TASK CONSIDERATION;
- WIDE USED FOR CLASSIFICATION TASKS;
- FAMILIAR TO THE SECURITY & SOCIAL SCIENCES.

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

The Key Idea of Morphological Analysis

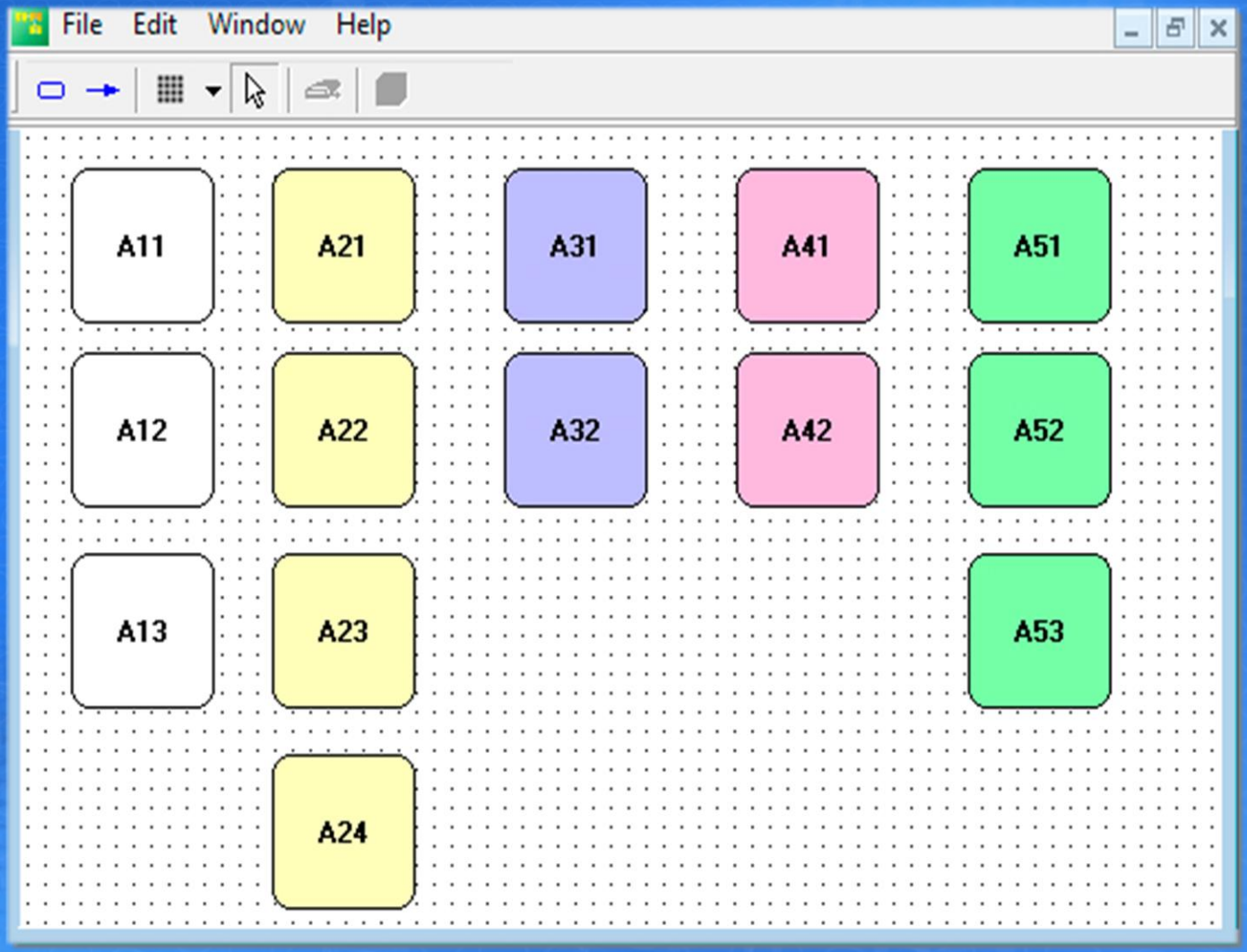
Dimensions

Alternatives	Dimension I	Dimension II	Dimension III
	A1,1	A2,1	A3,1
	A1,2	A2,2	A3,2
	A1,3	A2,3	A3,3
	A1,4		



This activity is supported by: The NATO Science for Peace and Security Programme

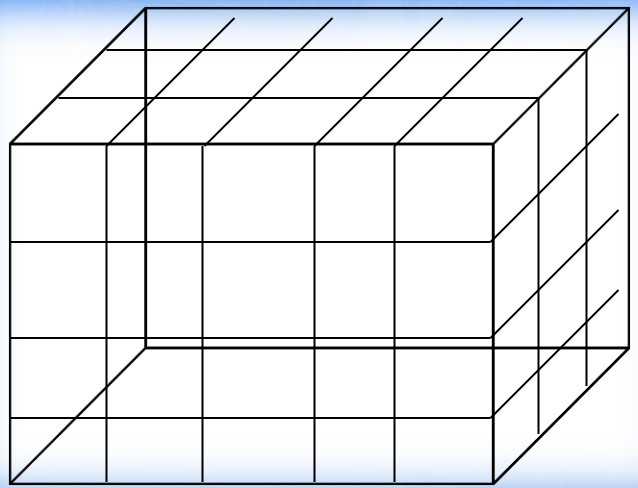
Step 1 Dimensions & alternatives definition



This activity is supported by: The NATO Science for Peace and Security Programme

General problem volume

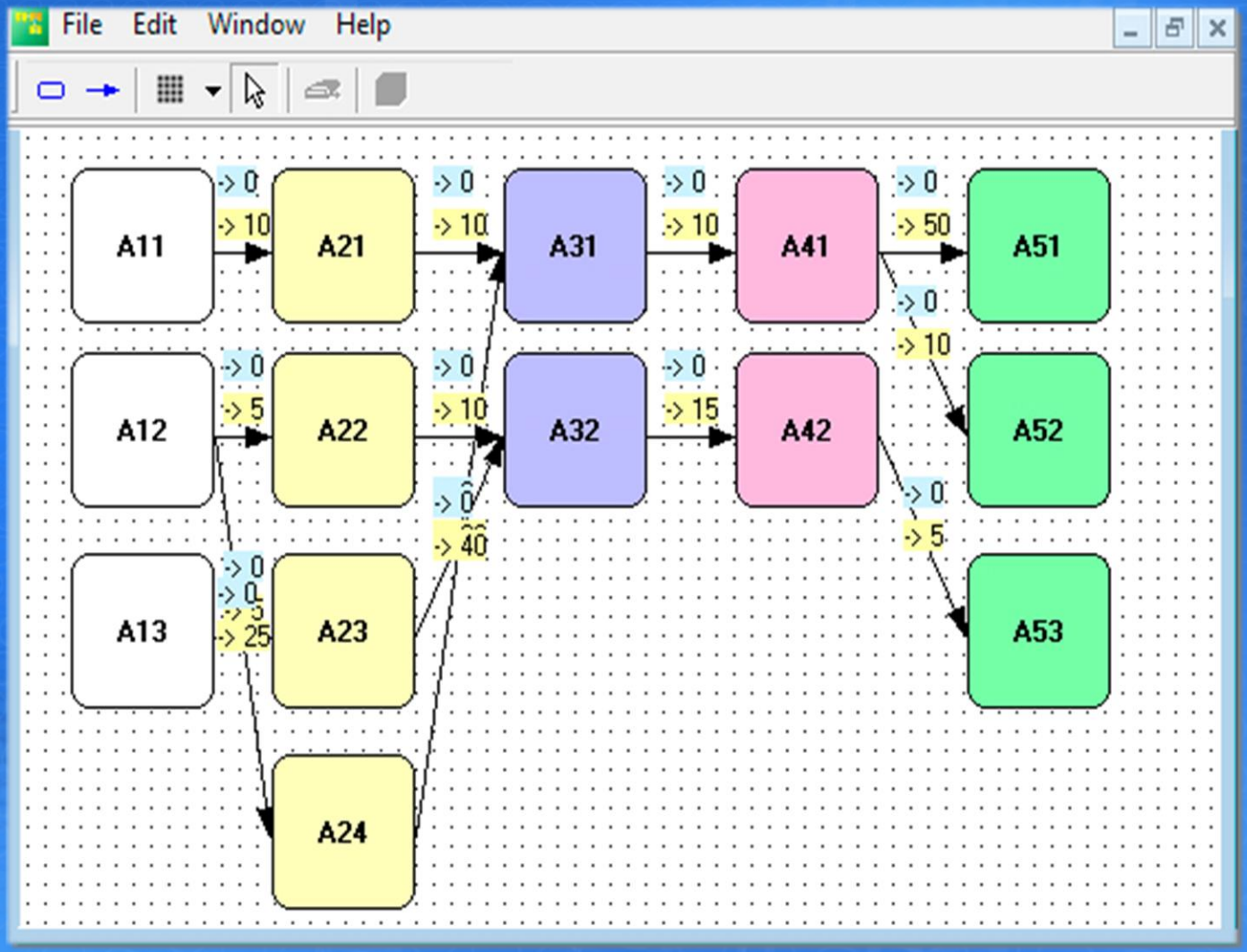
Possible combinations: 3 X 4 X 2 X 2 X 3 X 5 = 720



Driving factors are extremely necessary, otherwise you can not really optimize your resources!!!

NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Step 2 Alternatives binding



This activity is supported by: The NATO Science for Peace and Security Programme

Cross-consistency matrix

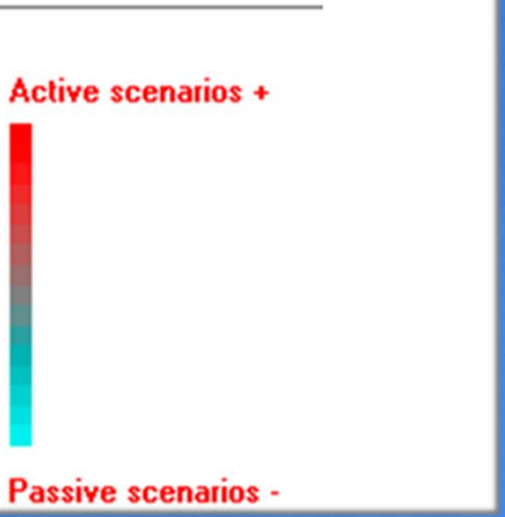
I	II	III	IV	V
A11	A21	A31	A41	A51
A12	A22	A32	A42	A52
A13	A23			A53
	A24			

NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Step 3 Scenario building, ranging & naming

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

Index	Length	Weight	Name
1	5	40	Scenario1
2	5	35	Scenario2
3	5	85	Scenario3
4	5	45	Scenario4
5	5	80	Scenario5
6	5	125	Scenario6



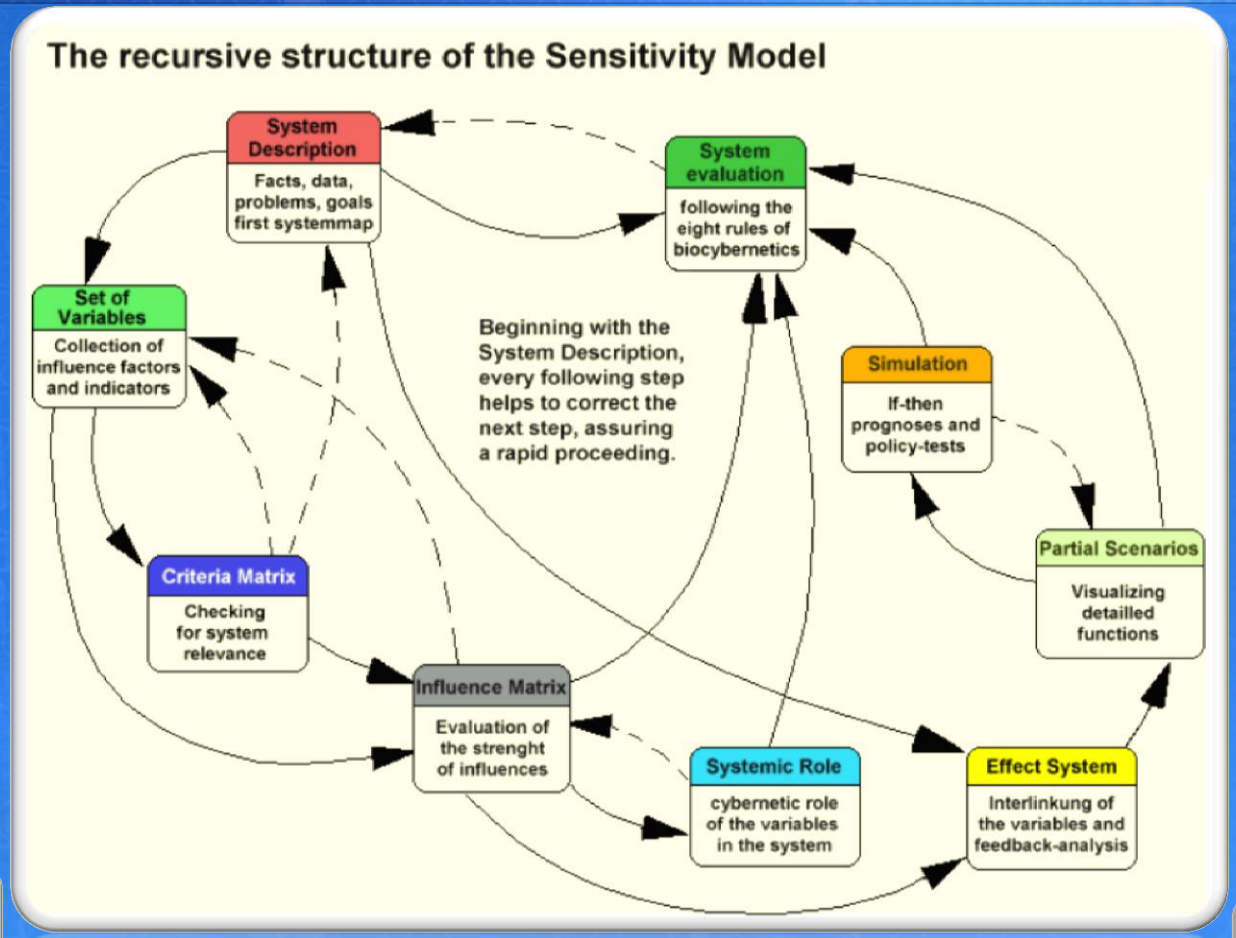
NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

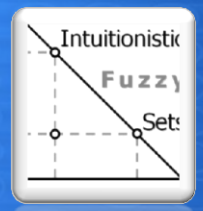
SYSTEM ANALYSIS

- INTUITIVE ENTITY-RELATIONSHIP NOTATION;
- DETAILS' CONSIDERATION;
- FAMILIAR TO THE MILITARY & SCIENTIFIC WORLD.

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

Implemented Ideas

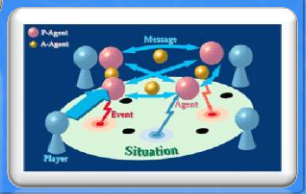




IFS decision support

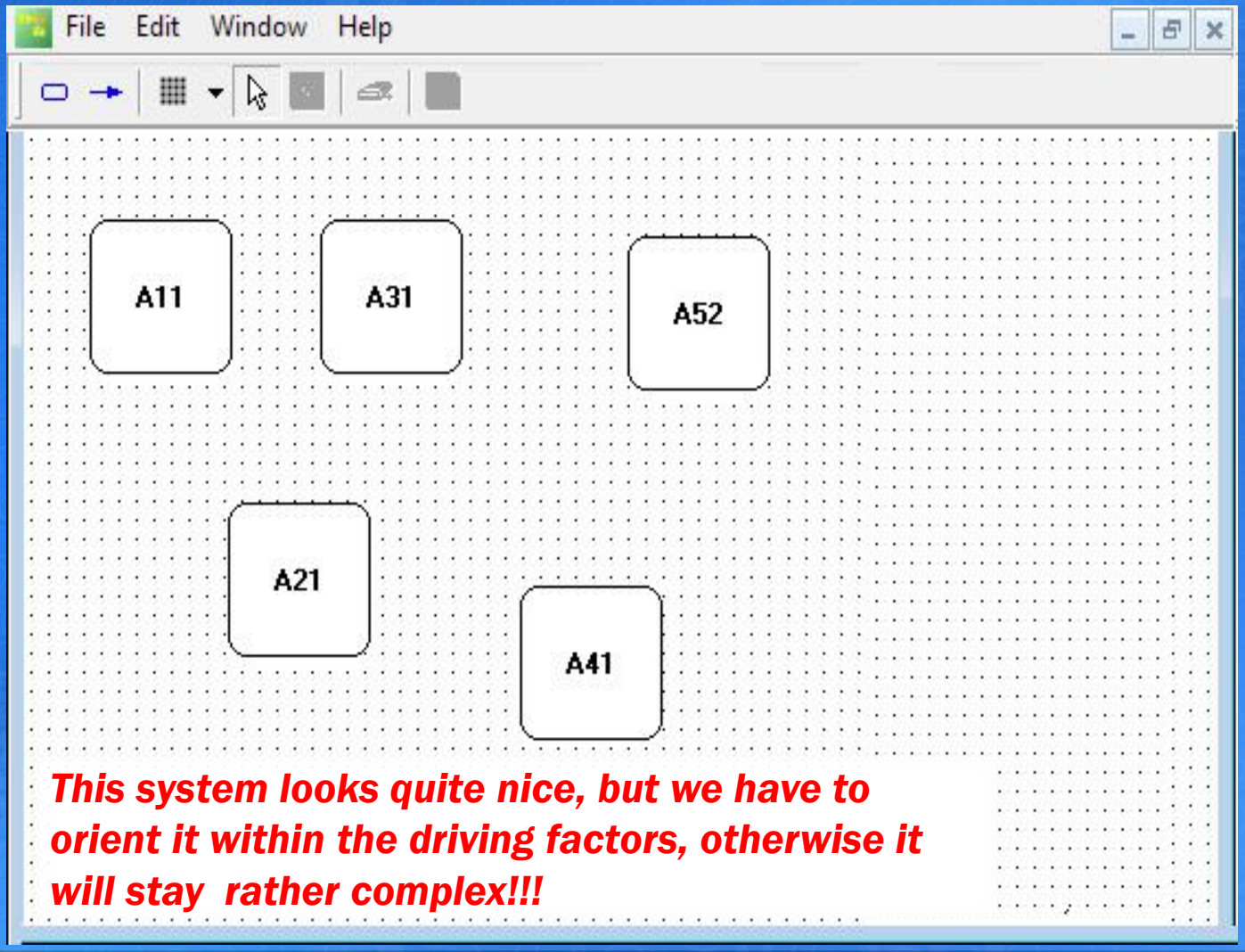
General System Theory

Multiagent representation



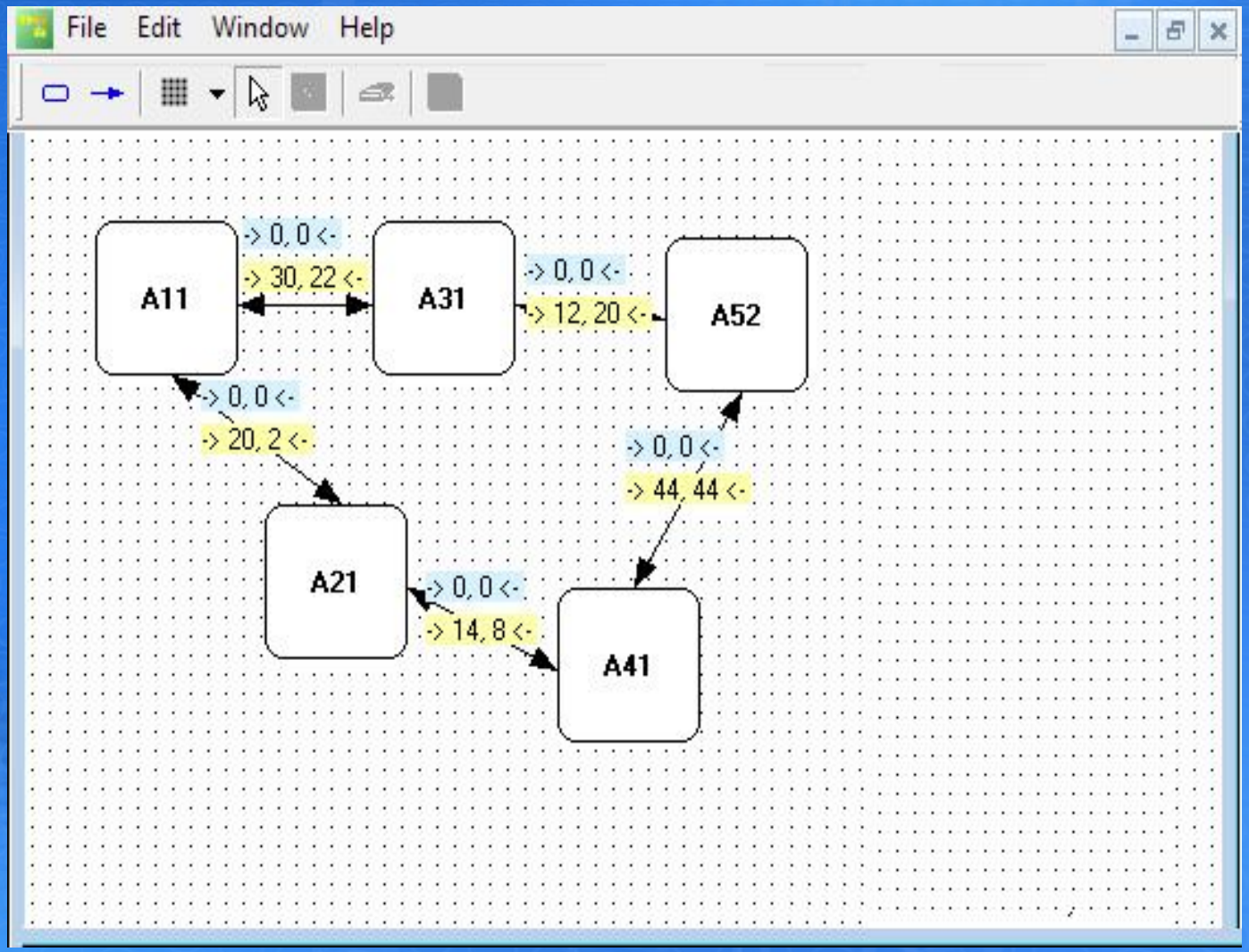
This activity is supported by: The NATO Science for Peace and Security Programme

Step 1 Entities definition



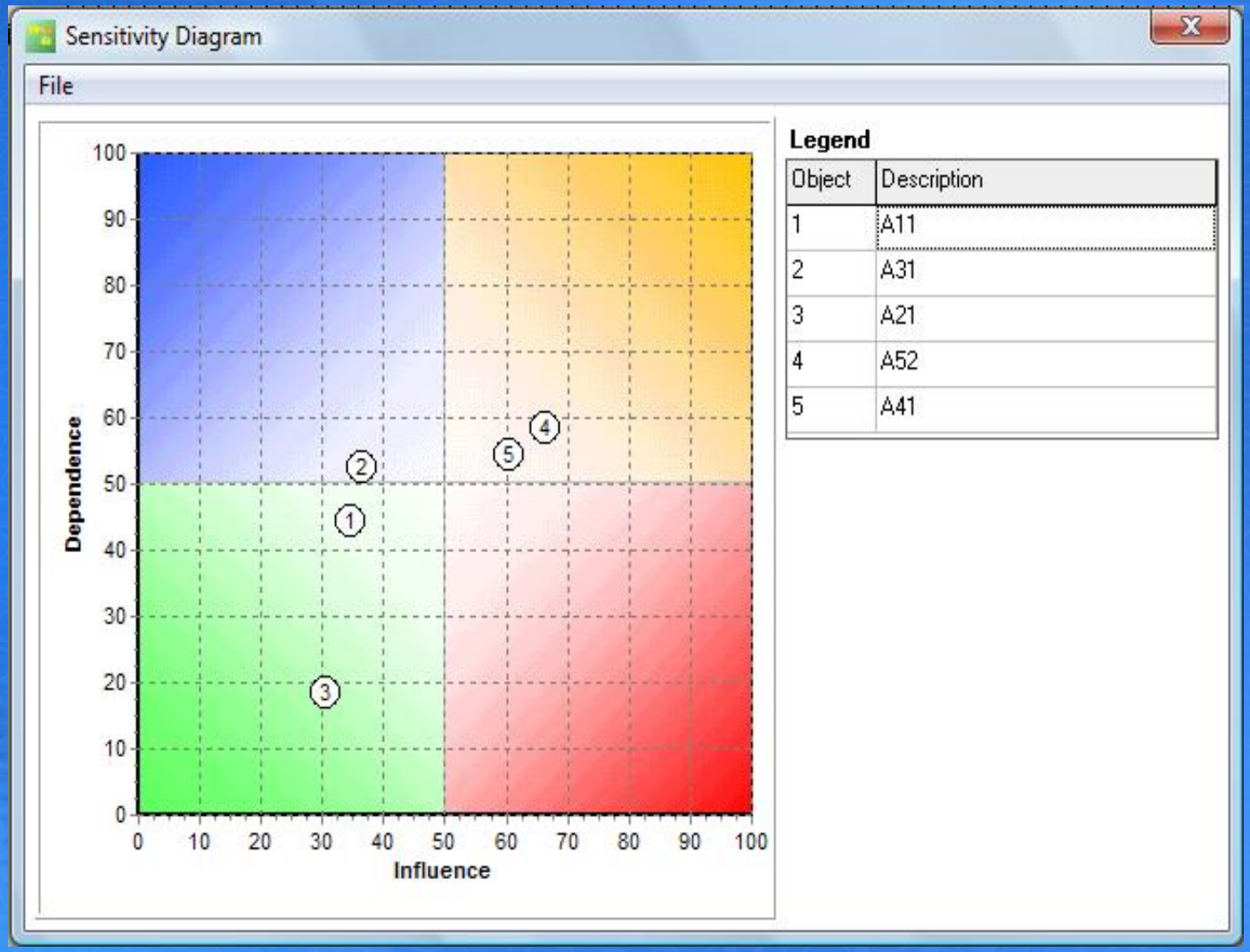
NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Step 2 Entities binding



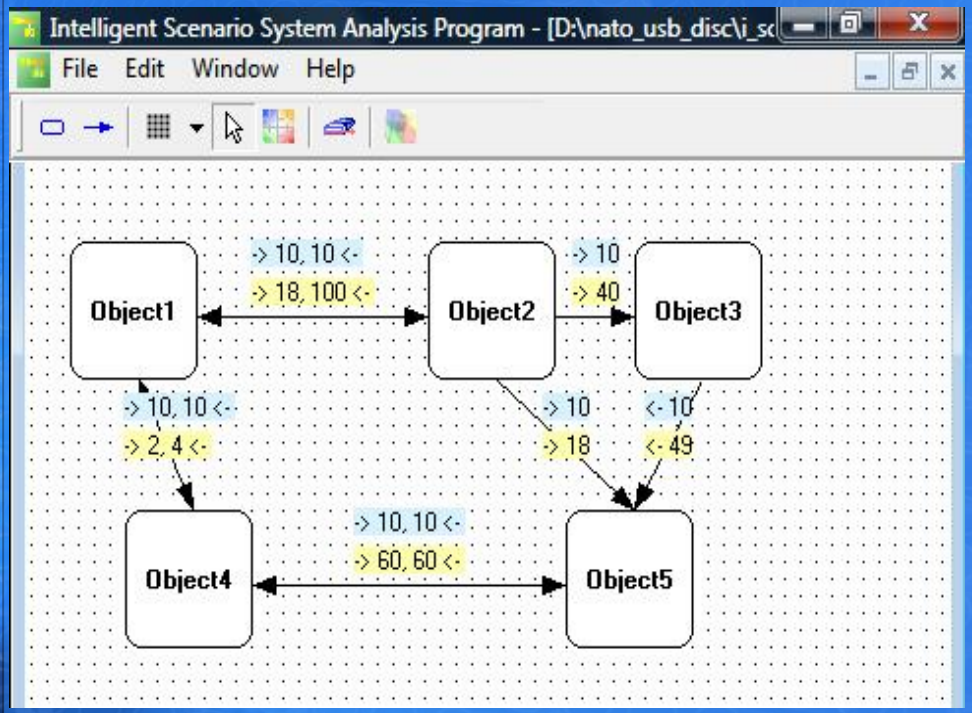
NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

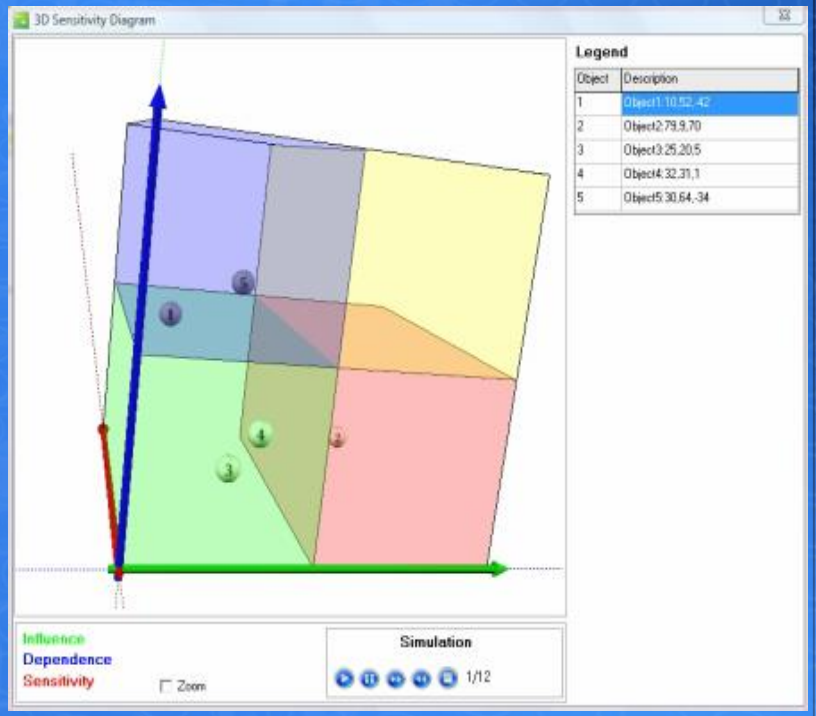
Step 3 Entities classification



This activity is supported by: The NATO Science for Peace and Security Programme

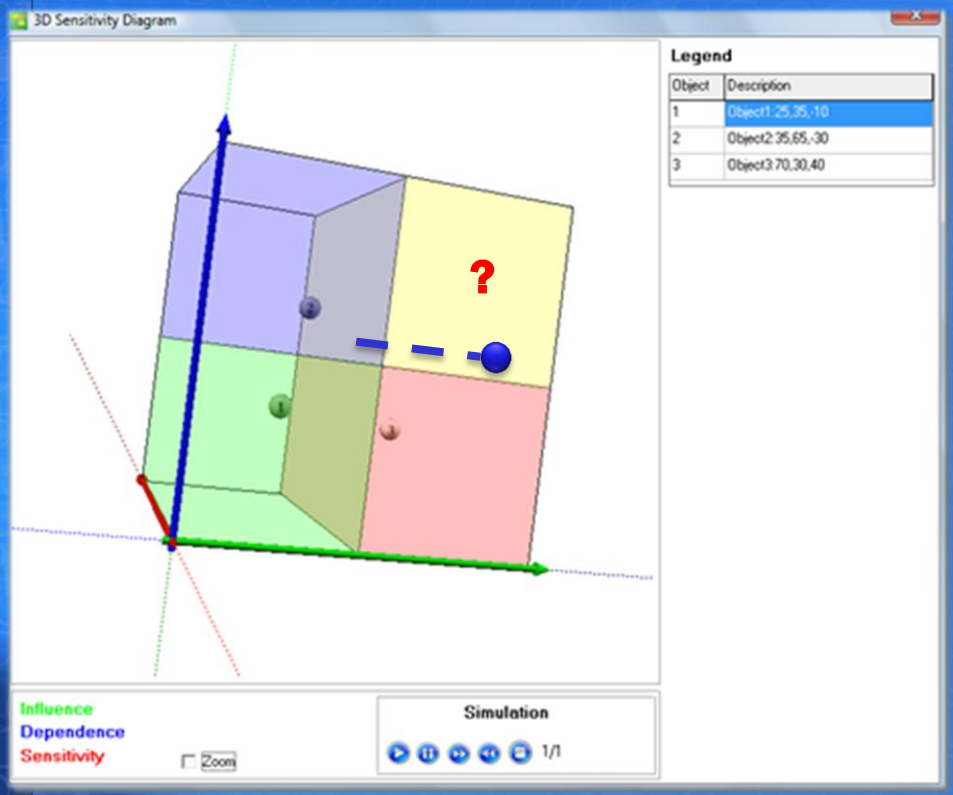
SENSITIVITY ANALYSIS IN 4D



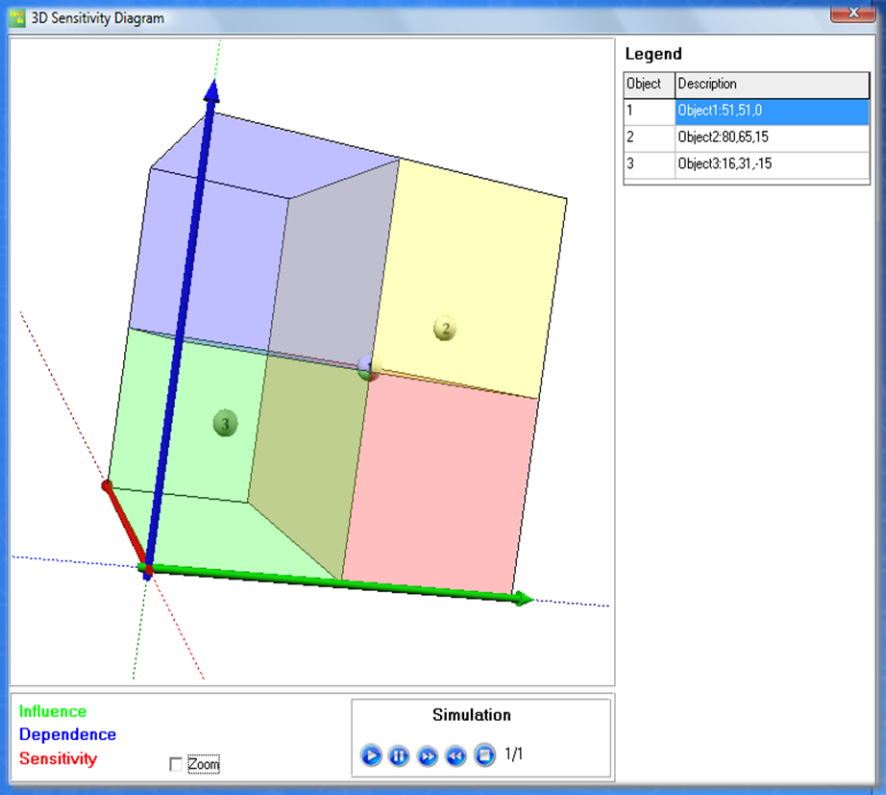


This activity is supported by: The NATO Science for Peace and Security Programme

But can we change the experts' believes with I-SCIP SD?



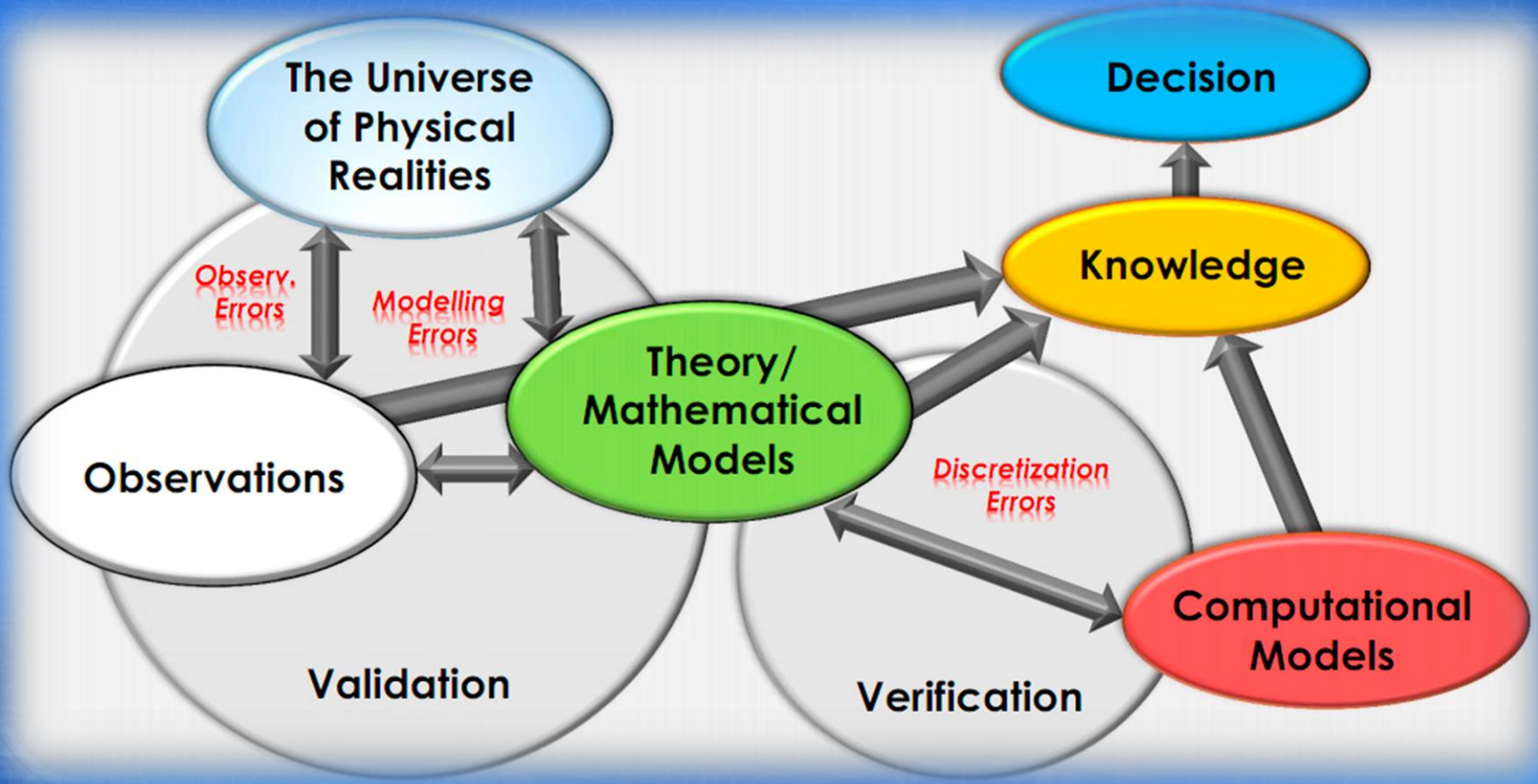
Initial Configuration



New Configuration after Q optimization

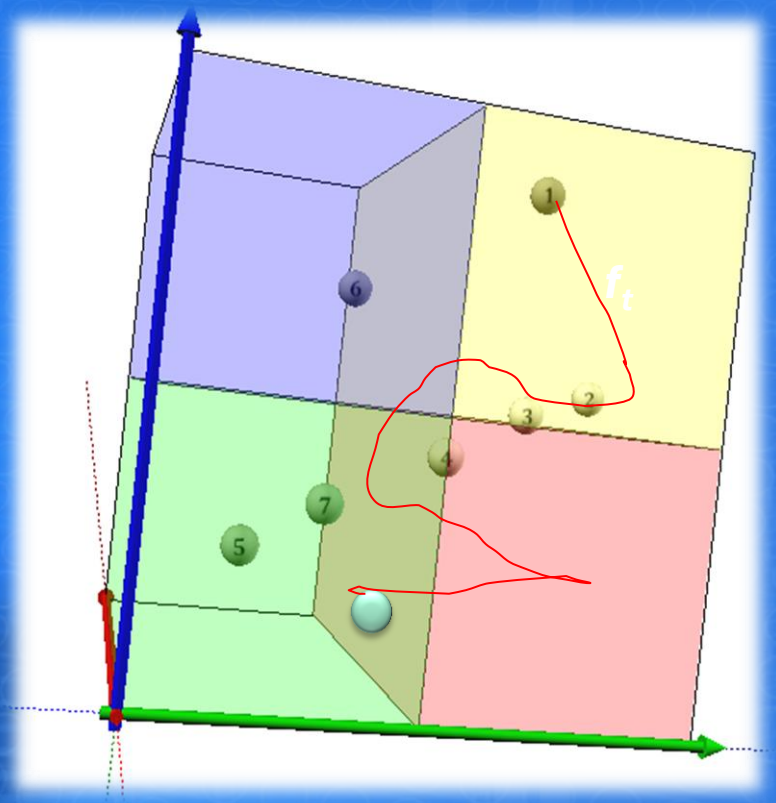
NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

And how certain we are?

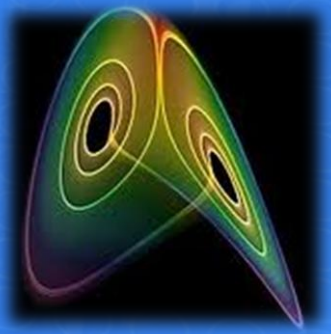


This activity is supported by: The NATO Science for Peace and Security Programme

THE TRANSITION FUNCTION IMPORTANCE & UNCERTAINTY

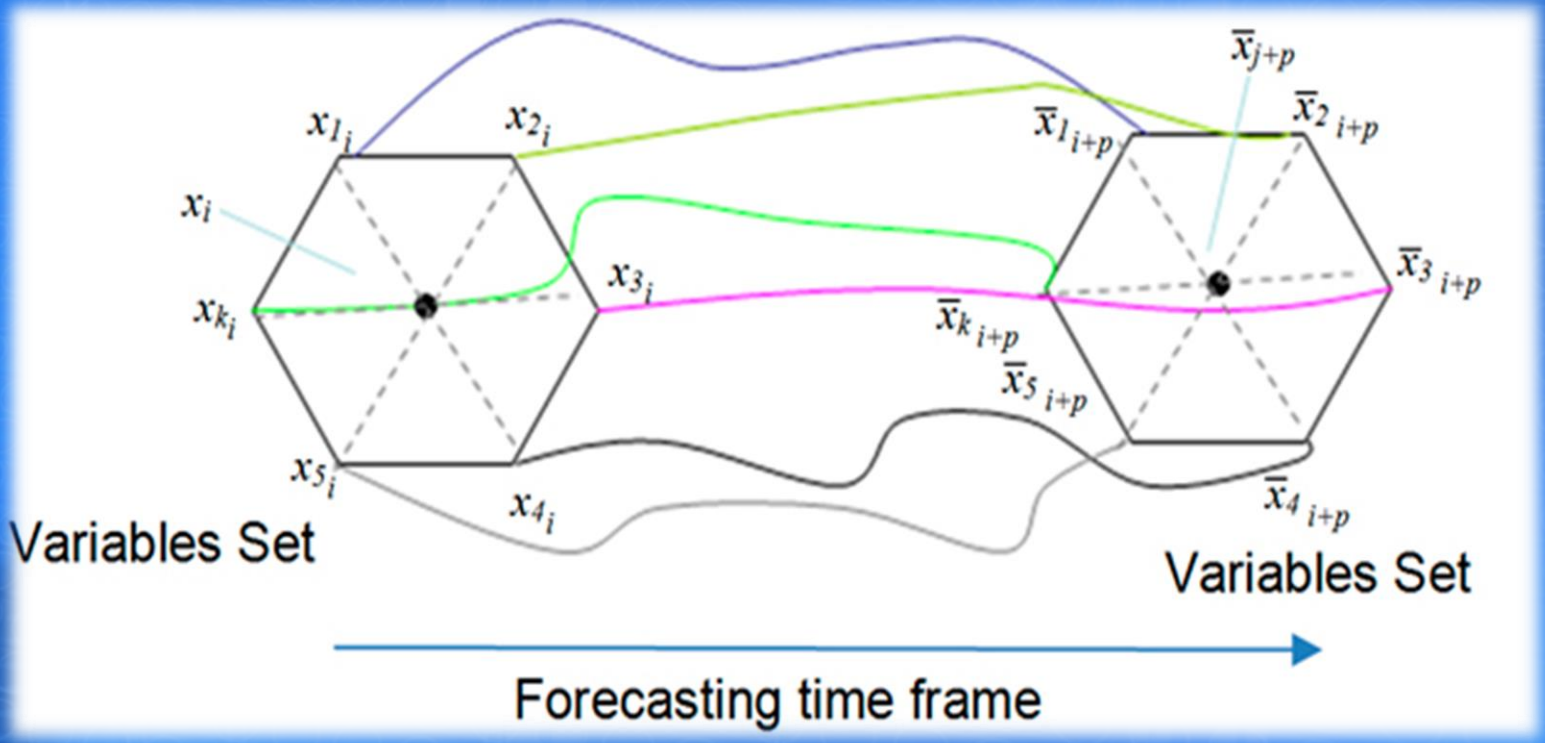


Example: f_t ~ **Lorenz system**



NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Mathematical Scenario Validation & Uncertainty Dynamics Monitoring

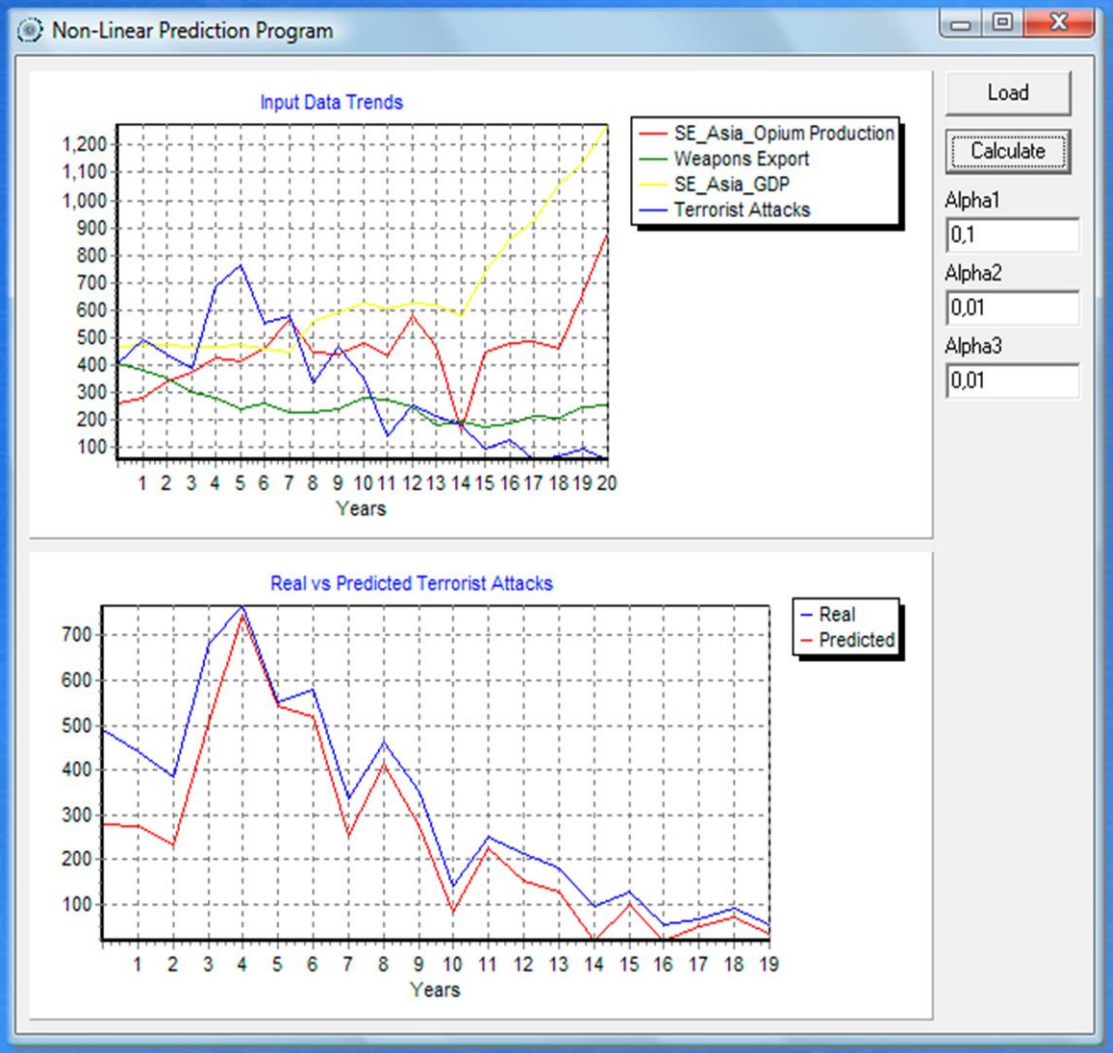


NATO OTAN

This activity is supported by:

The NATO Science for Peace and Security Programme

SOFTWARE SUPPORT

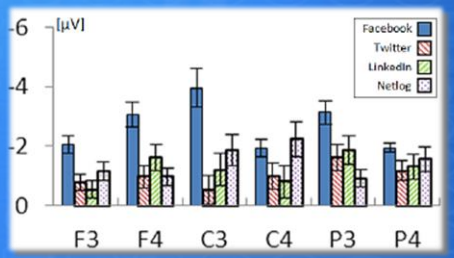


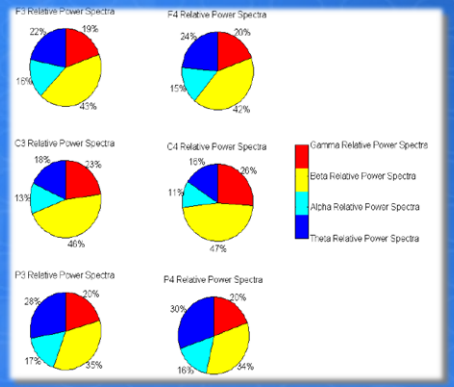
NATO OTAN

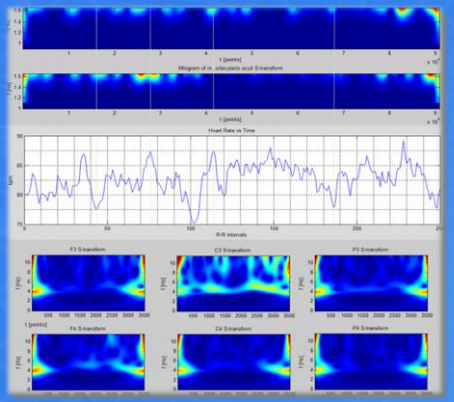
This activity is supported by:

The NATO Science for Peace and Security Programme

Psychophysiological Validation



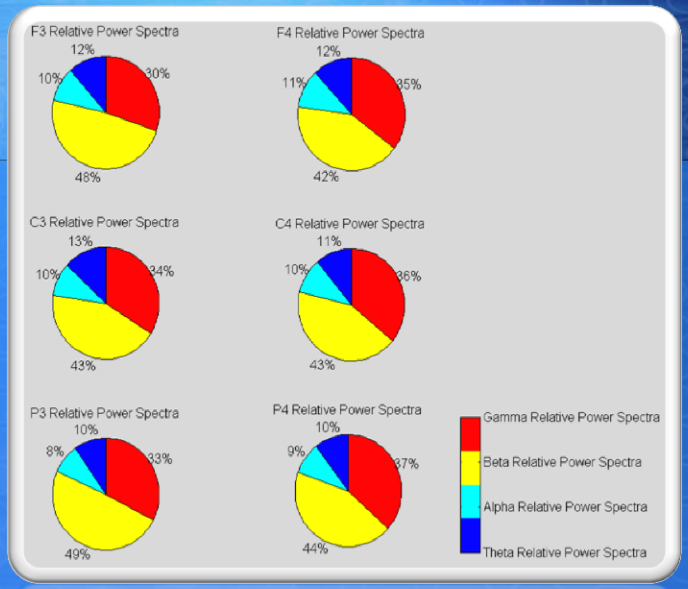




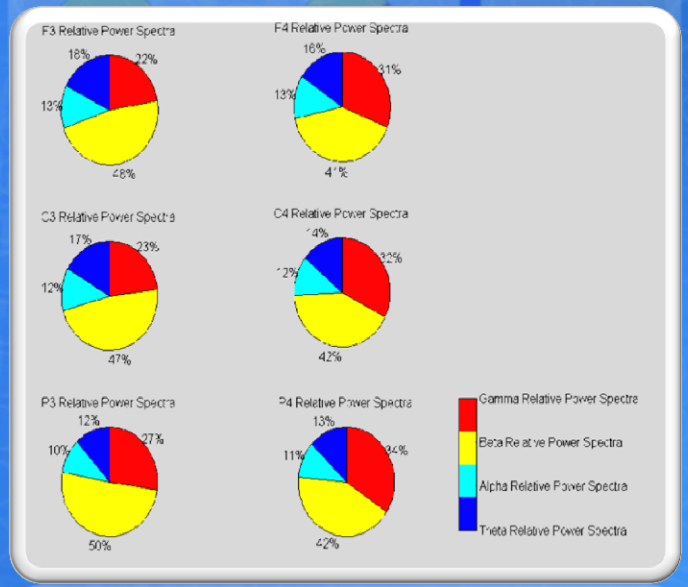
NATO OTAN

This activity is supported by: The NATO Science for Peace and Security Programme

2D



3D



NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Some Implementation Examples

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

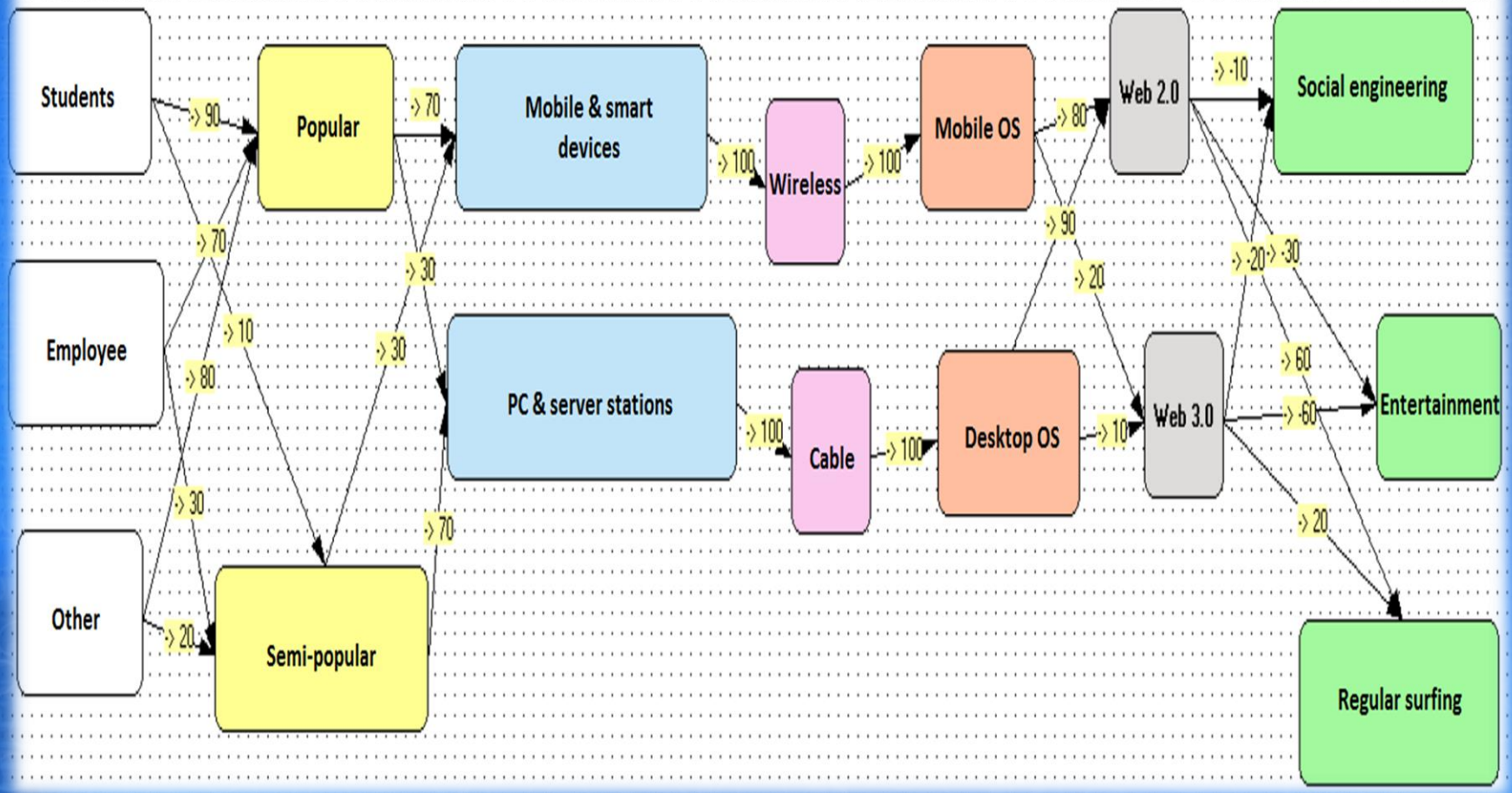
A Study on IT Threats and Users Behaviour Dynamics in Online Social Networks, DMU03/22, 2011-2014

www.snfactor.com

This activity is supported by: The NATO Science for Peace and Security Programme

Social networks context MA

Maximum scenario combinations: 7 X 3 X 2 X 2 X 2 X 2 X 2 X 3 = 2016



NATO OTAN

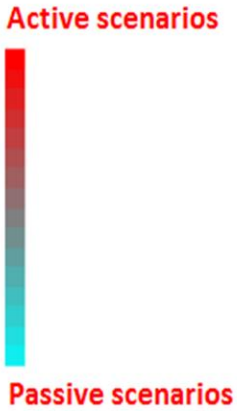
This activity is supported by: The NATO Science for Peace and Security Programme

Resulting Scenarios

Morphlogical analysis

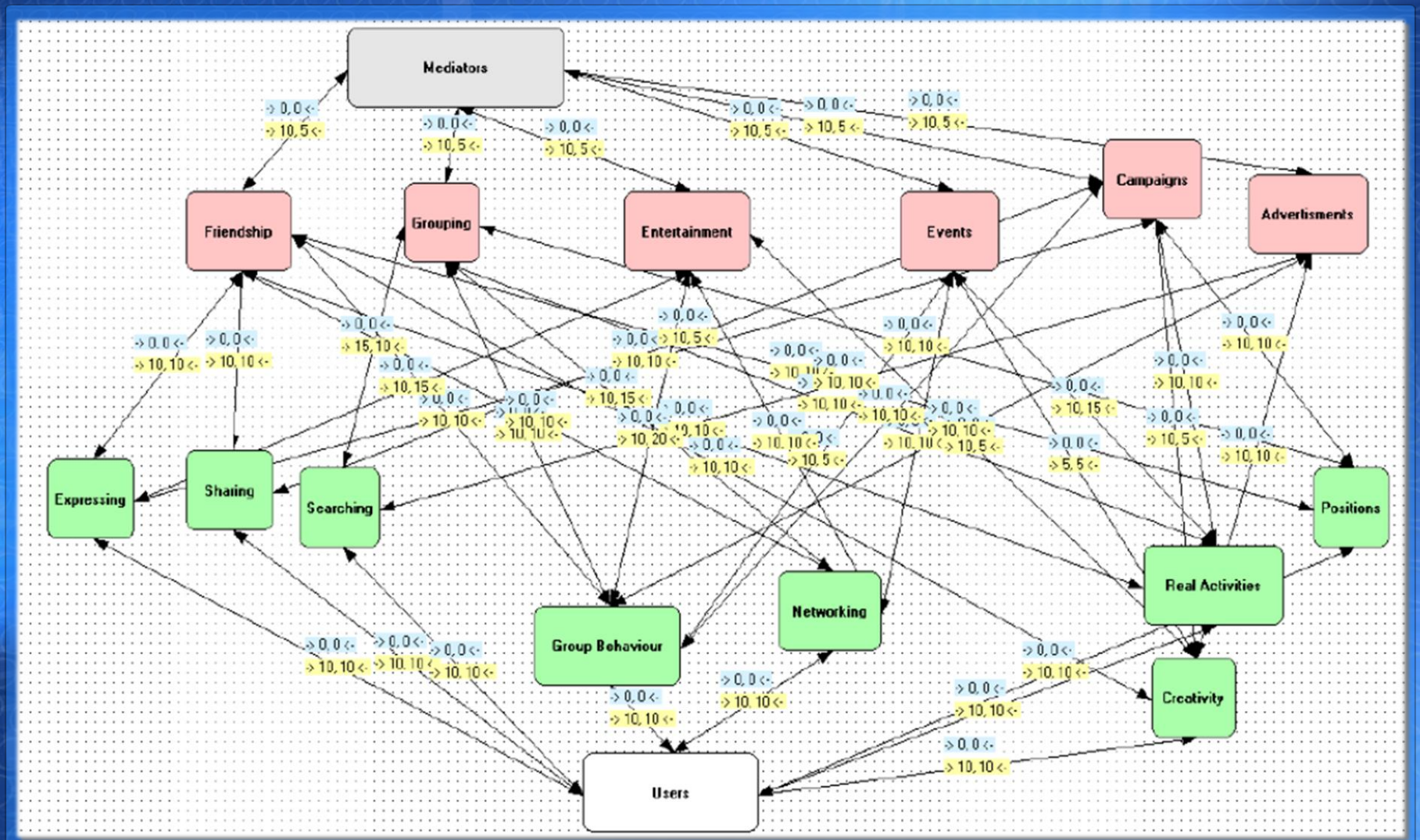
Users	*Social networks*	*Hardware technologies*	*Comms*	*Software platforms*	*Web standards*	*Activities*
Students	Popular	Mobile & smart devices	Wireless	Mobile OS	Web 2.0	Social Engineering
Emploee	Semi-popular	PC & server stations	Cable	Desktop OS	Web 3.0	Entertainment
Other						Regular surfing

Index	Length	Weight	Name
53	7	460	Scen.53
54	7	510	Scen. 54
55	7	490	Scen.55
56	7	470	Scen. 56
57	7	480	Scen.57
58	7	400	Scen.58
59	7	420	Scen. 59
60	7	410	Scen. 60



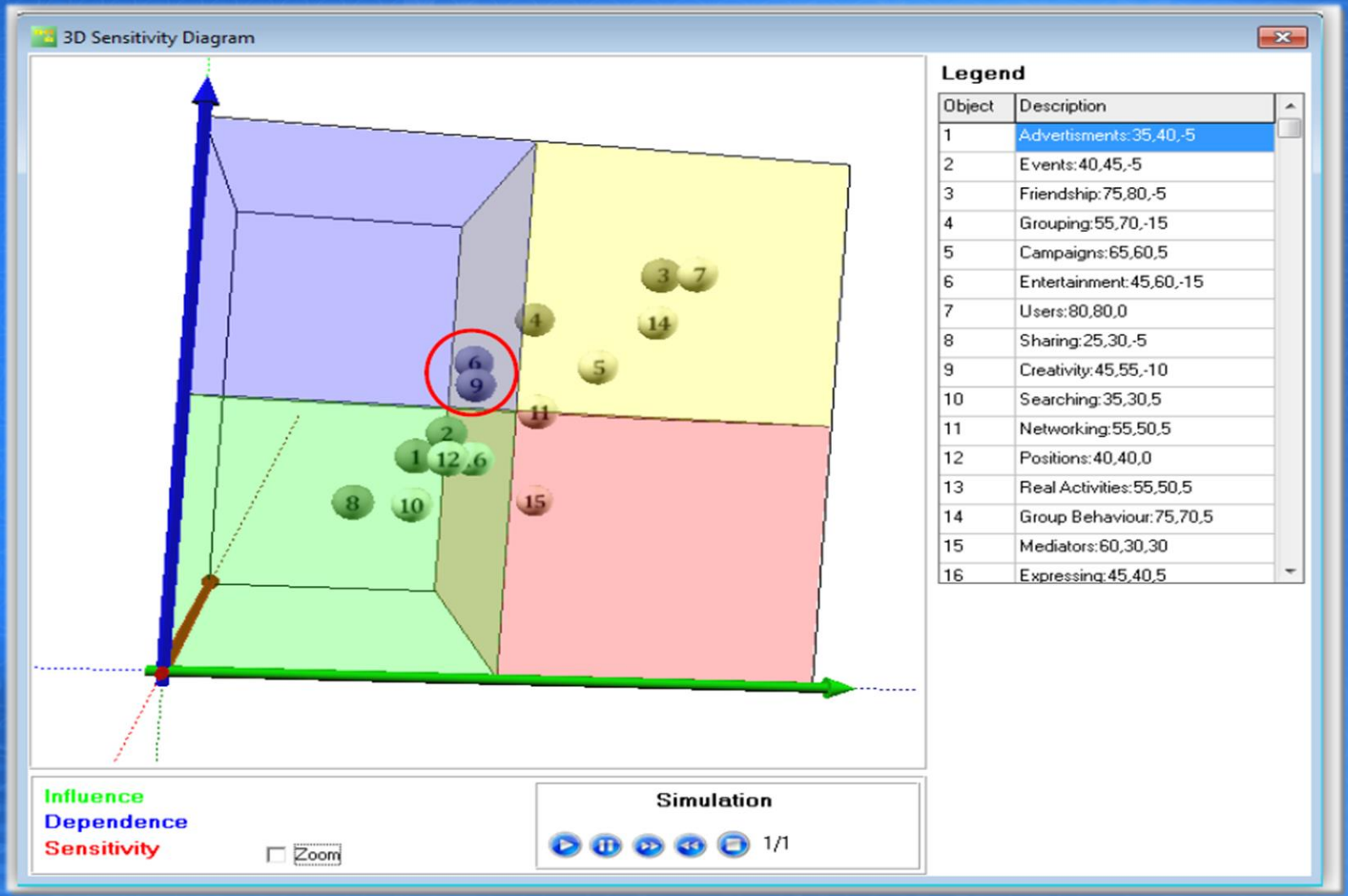
This activity is supported by: The NATO Science for Peace and Security Programme

Social Engineering SA



NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Sensitivity Diagram



This activity is supported by: The NATO Science for Peace and Security Programme

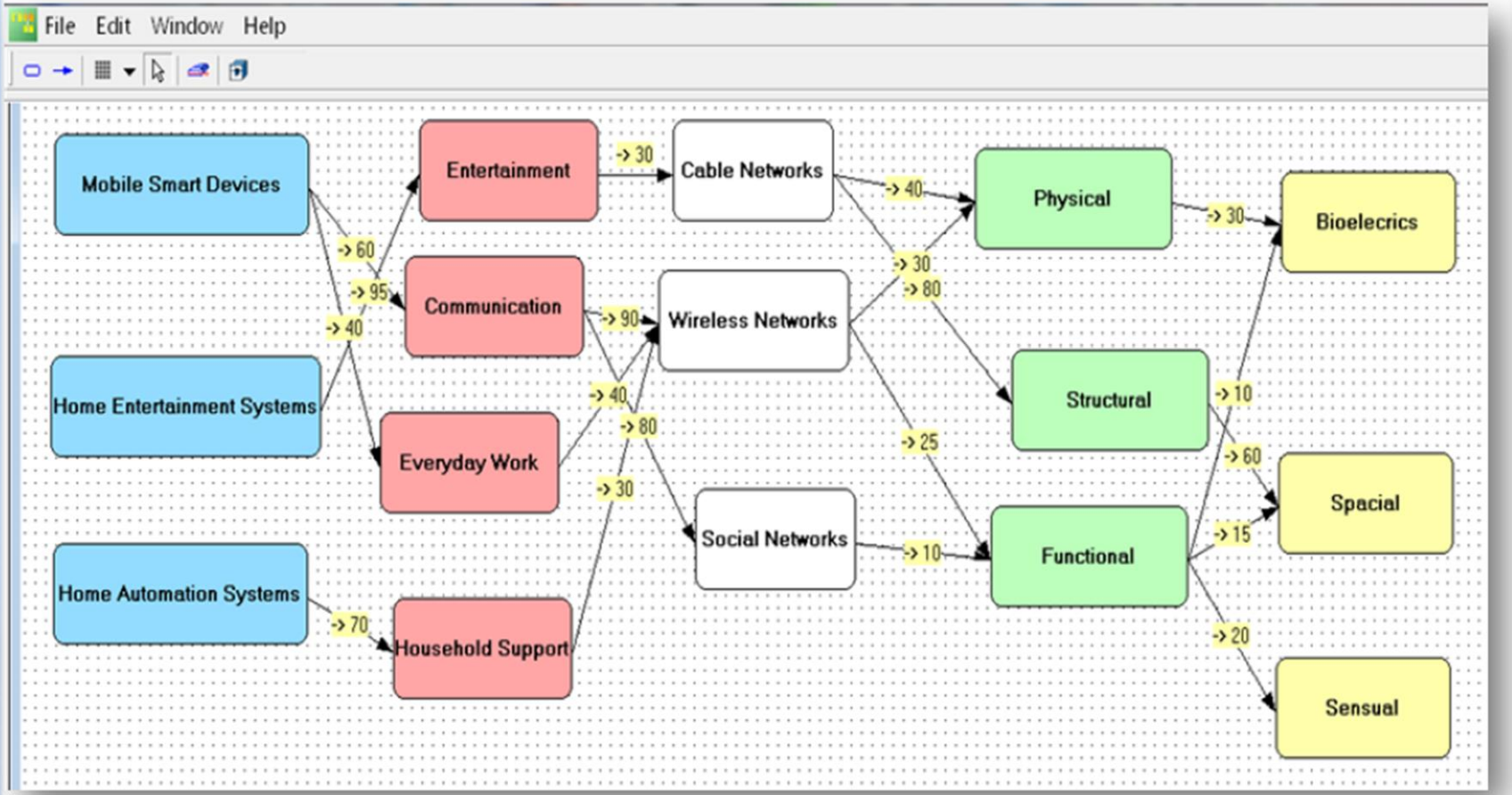
A Feasibility Study on Cyber Threats Identification and their Relationship with Users' Behavioural Dynamics in Future Smart Homes, DFNI-T01/4, 2012-2014

www.smarthomesbg.com

This activity is supported by: The NATO Science for Peace and Security Programme

Smarthomes context MA

MAXIMUM SCENARIO COMBINATIONS: 5x3x4x3x3x3 = 1620



NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

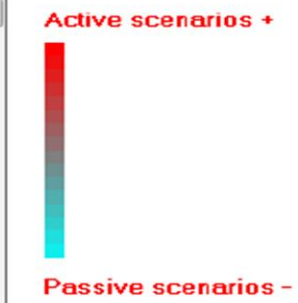
Resulting Scenarios

Selected Scenarios Set

Morphological Analysis

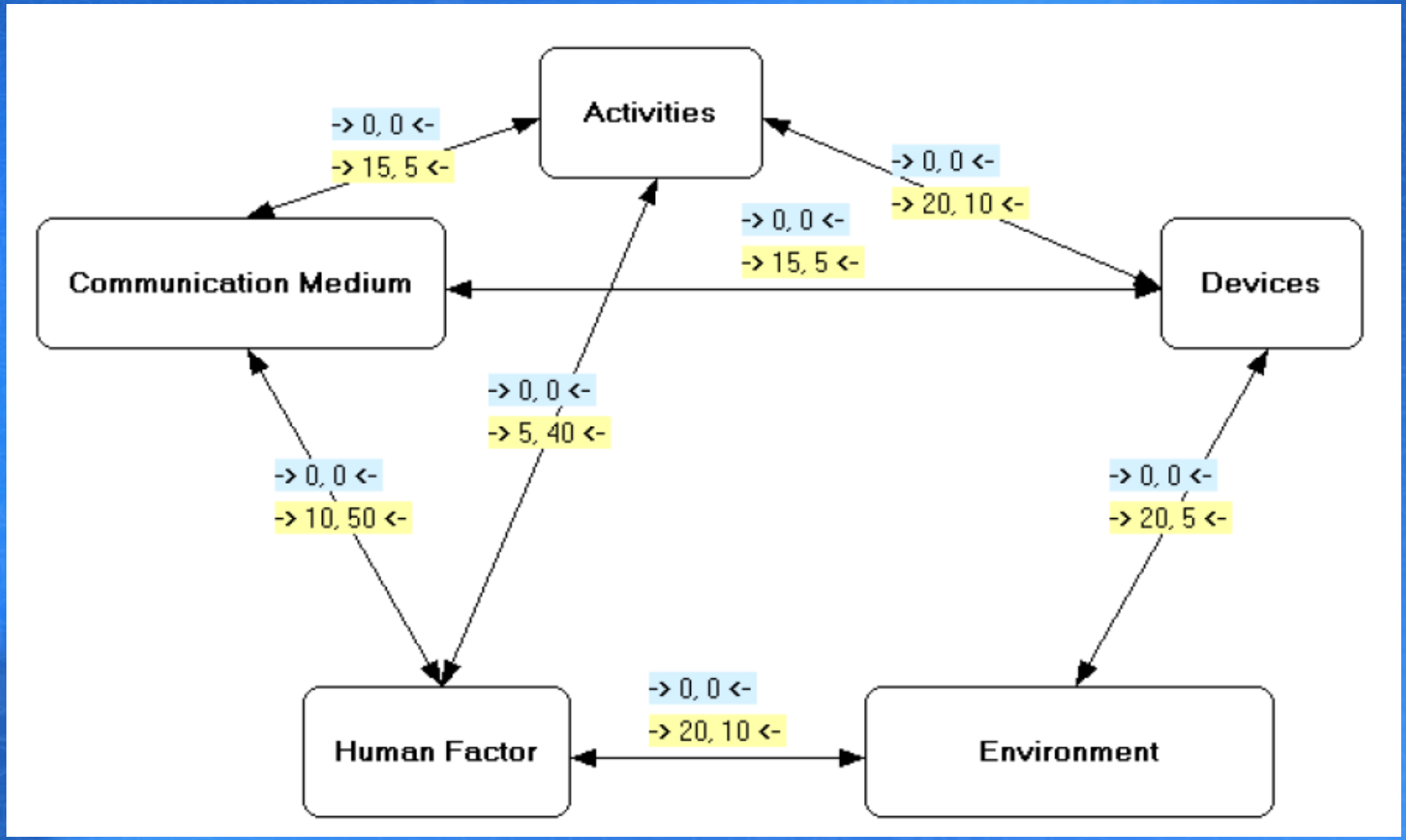
Devices	Activities	Communication Medium	Environment Characteristics	Human Factor Characteristics
Mobile Smart Devices	Entertainment	Cable Networks	Physical	Bioelectrics
Home Entertainment Systems	Communication	Wireless Networks	Structural	Spacial
Home Automation Systems	Everyday Work	Social Networks	Functional	Sensual
	Household Support			

Index	Length	Weight	Name
1	5	170	Scenario1
2	5	125	Scenario2
3	5	265	Scenario3
4	5	145	Scenario3
5	5	195	Scenario4
6	5	195	Scenario5
7	5	140	Scenario6
8	5	160	Scenario7
9	5	210	Scenario8
10	5	165	Scenario9
11	5	120	Scenario10
12	5	140	Scenario11



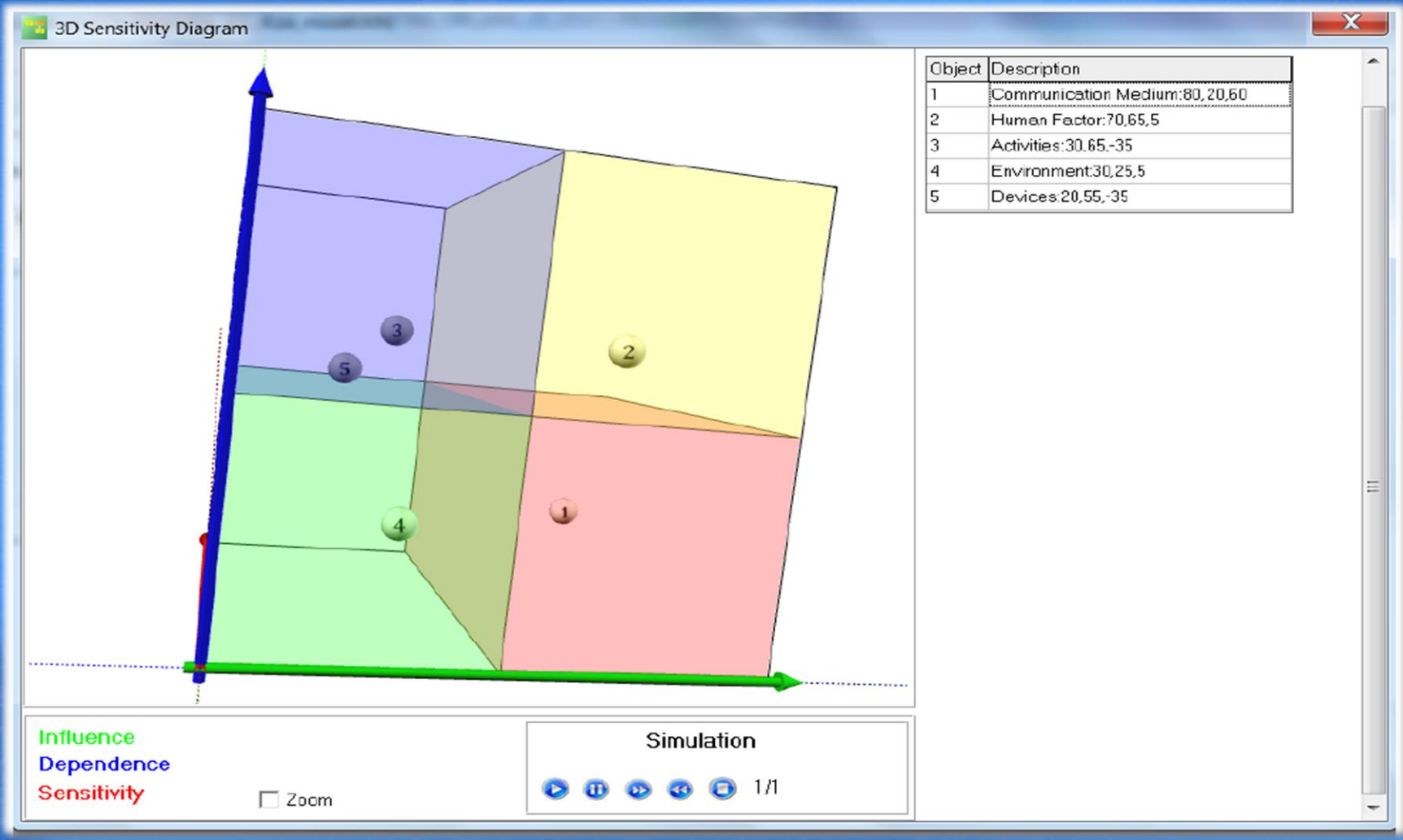
NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

General SA



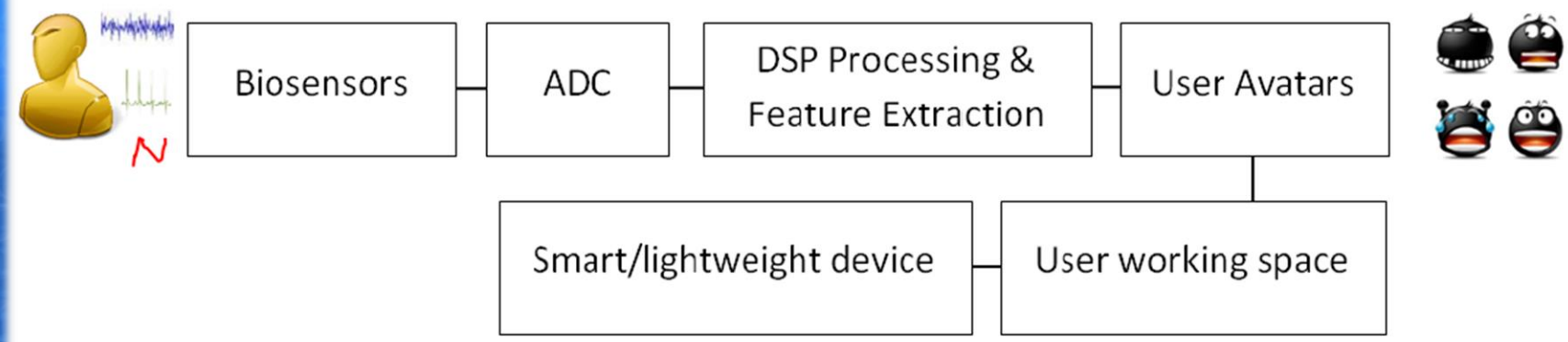
This activity is supported by: The NATO Science for Peace and Security Programme

Sensitivity Diagram



This activity is supported by: The NATO Science for Peace and Security Programme

Biofeedback & Profiling

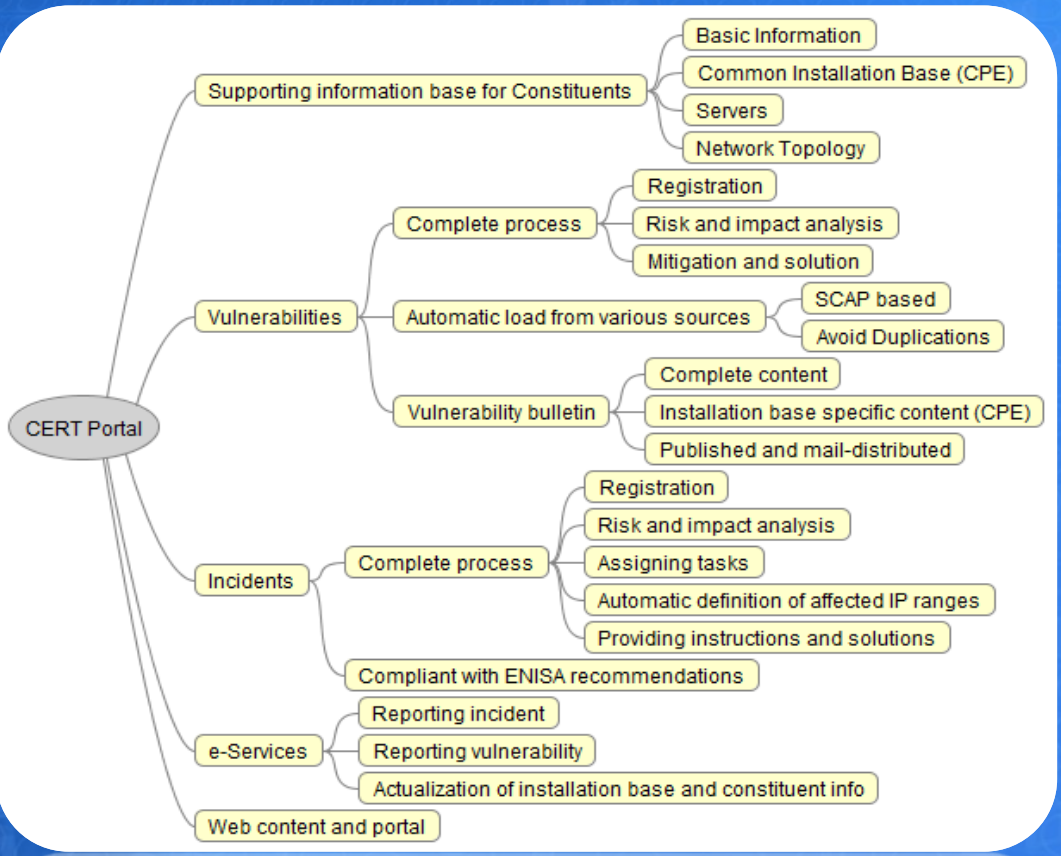


This activity is supported by: The NATO Science for Peace and Security Programme

Other Examples

This activity is supported by: The NATO Science for Peace and Security Programme

Bulgarian Cert Portal



www.govcert.bg

STEMO Computer Systems & Software

ESF Bulgaria
European Social Fund
Investing in people

This activity is supported by: The NATO Science for Peace and Security Programme

A European Network of Excellence in Managing Threats and Vulnerabilities for the Future Internet, SysSec, 2010-2014

- WP0: Management
- WP1: Dissemination
- WP2: Education
- WP3: Threats on the Future internet
- WP4: Malware and Fraud
- WP5: Smart Environments
- WP6: Cyberattacks

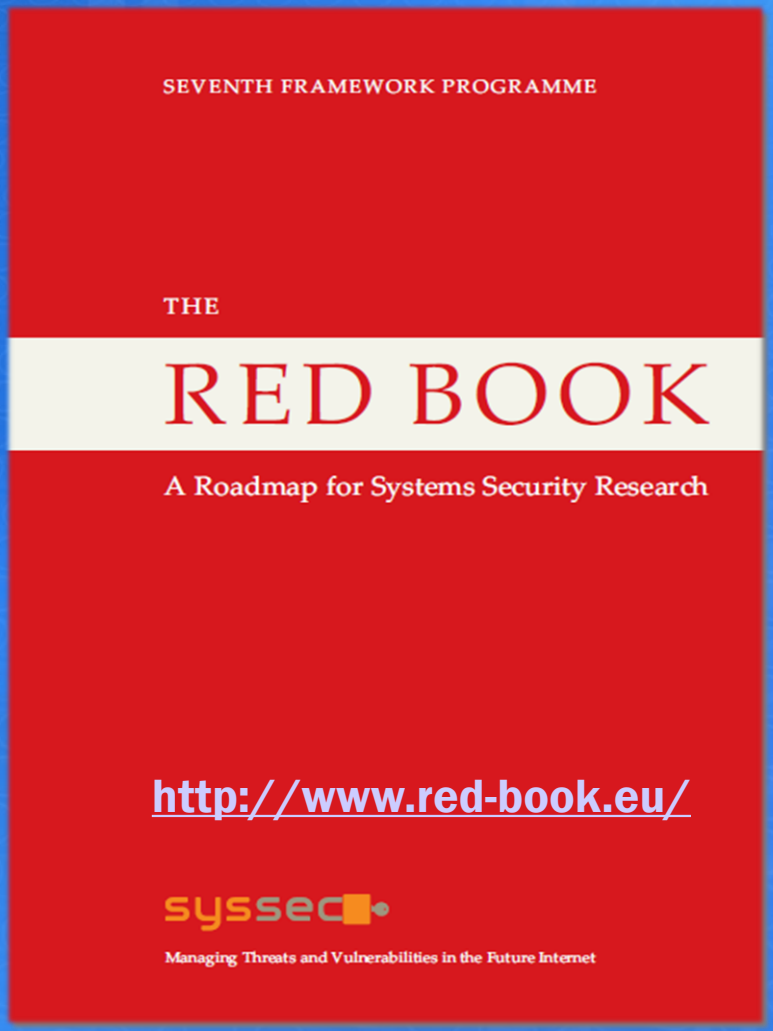
syssec

www.syssec-project.eu

NATO OTAN

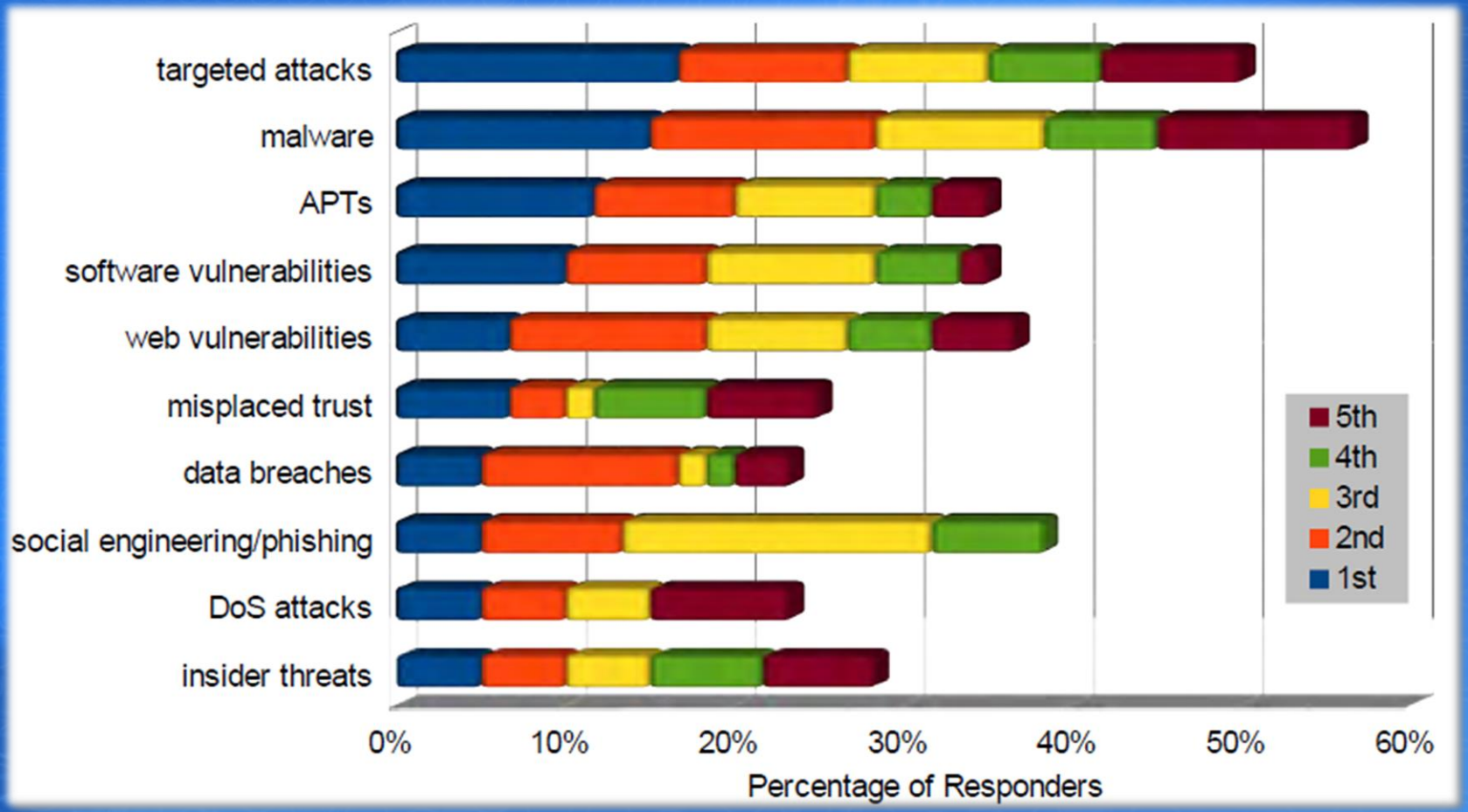
This activity is supported by: The NATO Science for Peace and Security Programme

A Roadmap for System Security Research 2013



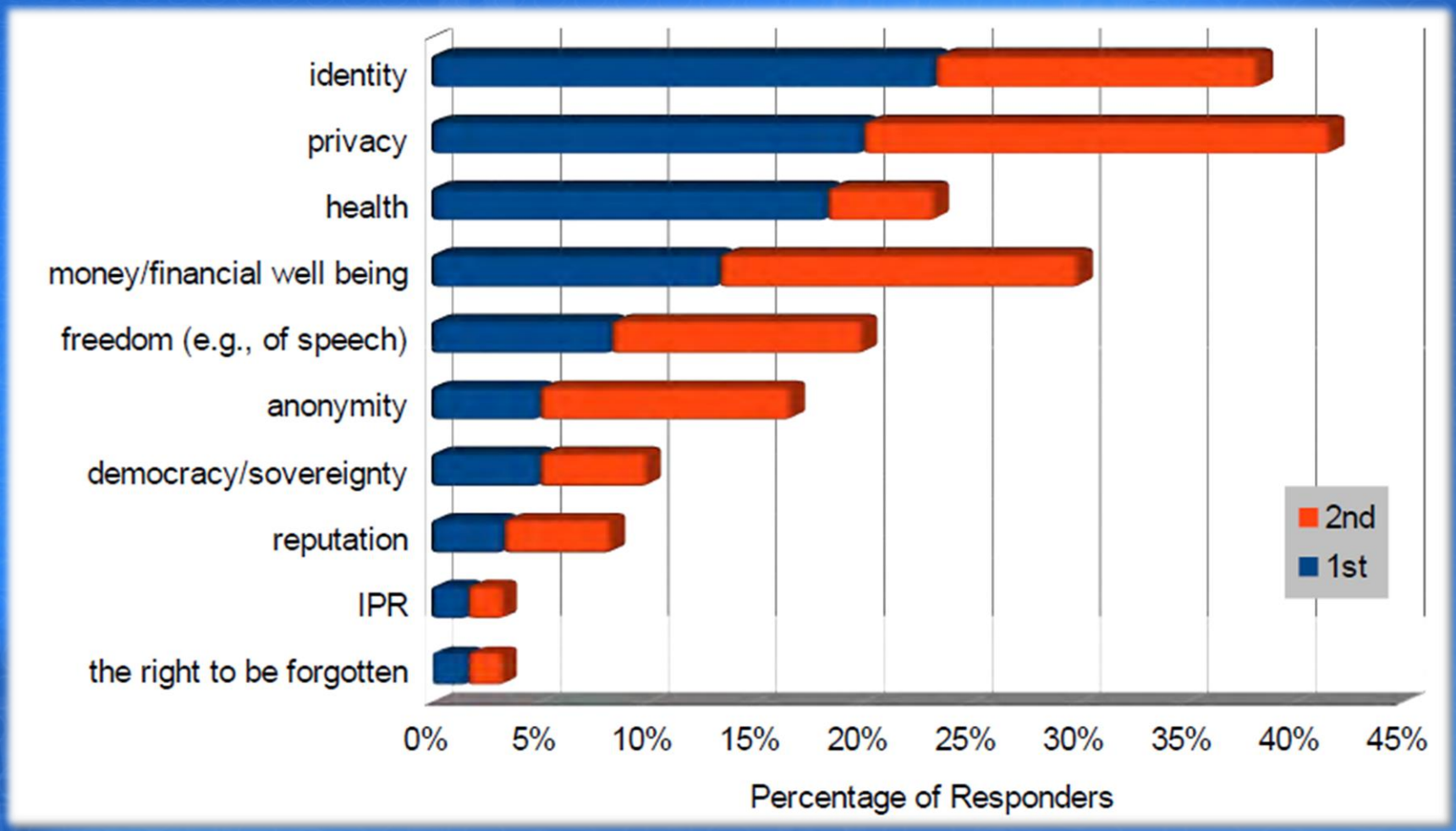
NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Mapping the threats we fear



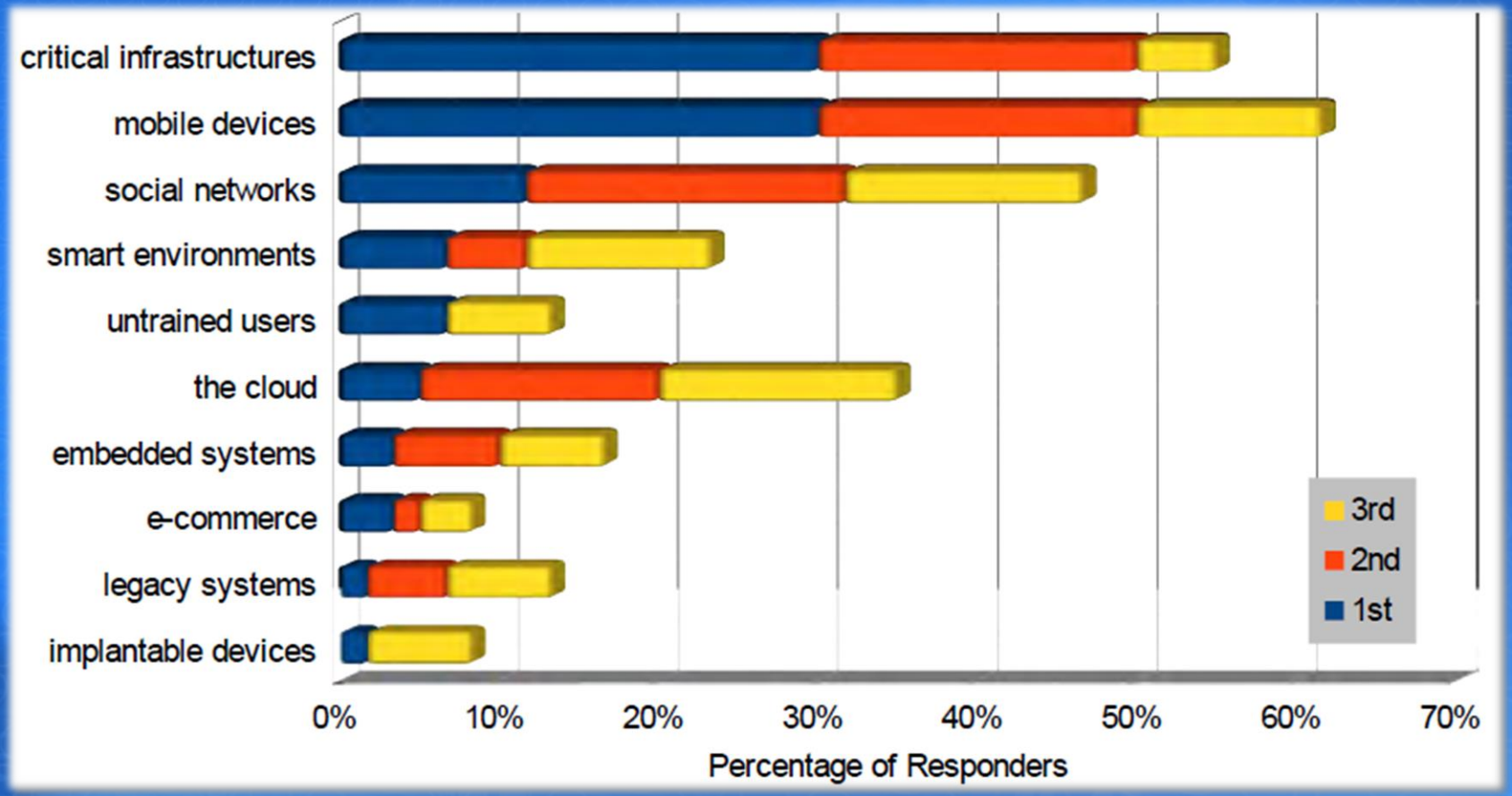
NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Listing the assets we value



NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

Domains of the game



NATO OTAN
This activity is supported by:
The NATO Science for Peace and Security Programme

In Summary

Threats

- Malware
- Targeted Attacks
- Social Engineering - Phishing

Domains

- Mobile Devices
- Social Networks
- Critical Infrastructures

Challenges

- No Device Should Be Compromisable
- Give Users Control Over Their Data
- Provide Private Moments in Public Places
- Develop Compromise-Tolerant Systems

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

Experimental Cyberthreats Brainstoriming

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

WHAT-IF SCENARIOS:

ROBOTS ENTER OUR EVERYDAY LIFE

HUMANS CAN ENTER THE VIRTUAL REALITY AND FEEL COMPLETELY THERE

HUMAN-MACHINE INTERACTION IS ALREADY AVAILABLE ON MENTAL LEVEL

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

THREATS & RISK BRAINSTORMING:

THREATS WE FEAR:

.....

DOMAINS:

.....

CHALLENGES:

.....

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

Discussion

Obviously, the identification of cyber risk and threats is not quite a trivial task. The presented methodological framework claims comprehensiveness by means of both the technological and human factor involvement. The analysis however is context dependent but at least manageable through validation!

So, there is no a universal solution but only a feasible one, because future forecasting has always been and still stays a challenge ☺

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme

ACKNOWLEDGEMENT

The presented results have been supported by the following projects: (1) "A Study on IT Threats and Users Behaviour Dynamics in Online Social Networks", DMU03/22, Bulgarian Science Fund, Ministry of Education Youth and Science, 2012-2014, www.snfactor.com; (2) EU Network of Excellence in Managing Threats & Vulnerabilities for the Future Internet, SysSec, 2010-2014, EU FP7, www.syssec-project.eu; (3) "A Feasibility Study on Cyber Threats Identification and their Relationship with Users' Behavioural Dynamics in Future Smart Homes", Bulgarian Science Fund, Ministry of Education Youth and Science, 2012-2014, DFNI-T01/4", www.smarthomesbg.com; (4) Cortical Regulation of the Quiet Stance during Sensory Conflict, Bulgarian Science Fund, Ministry of Education Youth and Science, TK 02/60, 2011-2014, www.cleverstance.com.

A special appreciation is also given to JTSAC longstanding academic & industrial partners: Institute of Mathematics & Informatics – Bulgarian Academy of Sciences, Institute of Neurobiology-Bulgarian Academy of Sciences, STEMO Ltd, ADEA Ltd. and VISENSI Ltd.

Finally, the author expresses gratitude to the organizers and sponsors of NATO Regional Summer School on Cyberdefence, 20-26 October, 2013, Ohrid, Macedonia for the great opportunity of sharing experience and ideas.

Selected References

- Minchev, Z. Cyber Threats in Social Networks and User's Response Dynamics, IT4SEC Report 105, December, 2012, Available at: http://www.it4sec.org/bg/system/files/IT4Sec_Reports_105_2.pdf

- Minchev, Z., Boyanov, L., & Georgiev, S. Security of Future Smart Homes. Cyber-Physical Threats Identification Perspectives, National conference with international participation in realization of the EU project 'Development of Tools Needed to Coordinate Inter-sectorial Power and Transport CIP Activities at a Situation of Multilateral Terrorist Threat. Increase of the Capacity of Key CIP Objects in Bulgaria', at Grand Hotel 'Sofia', Sofia city, Bulgaria, June 4, 2013, Available at: http://smarthomesbg.com/files/dfni_t01_4_zm_lb_sg_paper_bulcip_proj_conf_june_2013.pdf

- Zlatogor Minchev, Plamen Gatev. Psychophysiological Evaluation of Emotions due to the Communication in Social Networks. In Scripta Scientifica Medica, Volume 44, Issue 1, Supplement 1. April 2012, Available at: http://www.syssec-project.eu/media/page-media/3/zm-pg-ssm-2012.pdf

NATO OTAN

This activity is supported by: The NATO Science for Peace and Security Programme

- Minchev, Z. CAX application for simulation and training in support of CIMIC. The Bulgarian academic experience, Amsterdam, the Netherlands, MCC 2011 Conference, October 17-18, 2011, Published in Military Communications and Information Technology: A Comprehensive Approach Enabler, Military University of Technology, Warsaw, Poland, 71-81, 2011.

- Minchev, Z., Shalamanov, V., Scenario Generation and Assessment Framework Solution in Support of the Comprehensive Approach, In Proceedings of SAS-081 Symposium on "Analytical Support to Defence Transformation", RTO-MP-SAS-081, Sofia, Boyana, April 26 – 28, 22-1 – 22-16, 2010.

- EU Network of Excellence in Managing Threats & Vulnerabilities for the Future Internet, SysSec Project Web Page: www.syssec-project.eu

- Study of the Information Threats and Behavior Dynamics of Social Networks Users from the Internet, DMU03/22 Project Web Page: http://snfactor.com

NATO OTAN

This activity is supported by: The NATO Science for Peace and Security Programme

THANK YOU FOR THE ATTENTION!

QUESTIONS?

NATO OTAN
This activity is supported by: The NATO Science for Peace and Security Programme