# Cyber Threats Identification Framework for Future Smart Homes

**Luben Boyanov & Zlatogor Minchev**

*Institute of ICT, Bulgarian Academy of Sciences*


NATO Advanced Research Workshop –
"Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework"

June 10-12, 2013 Ohrid, Macedonia

# Contents

- Cyber threats and smart homes
- Approach to treats identification
- Implementation and examples
- Resulting scenarios
- Ongoing and future work

# DIGITAL WORLD



# CYBER THREATS

- DIGITAL SOCIETY IS NO LONGER A TOPIC OF THE FUTURE OR SCIENCE FICTION BOOKS, BUT A REALITY OF TODAY;

- IN ADDITION TO THE BENEFITS THAT IT PROVIDES TO THE PEOPLE, IT ALSO COMES WITH A NUMBER OF ISSUES AND PROBLEMS, ONE OF THE MOST IMPORTANT OF WHICH IS SECURITY;

- THERE HAVE BEEN AN EXPANSION OF THE TRADITIONAL THREATS INTO NEW FIELDS LIKE SOCIAL MEDIA AND MOBILE DEVICES;

- ONLINE ABUSE AND CRIME IS SPREADING NOT ONLY FOR THE "TRADITIONAL" BUSINESS AND BANKING BUT ALSO TO NEW PLATFORMS, EMERGING WITH THE NEW TECHNOLOGIES AND APPLICATIONS.

# SMART HOMES

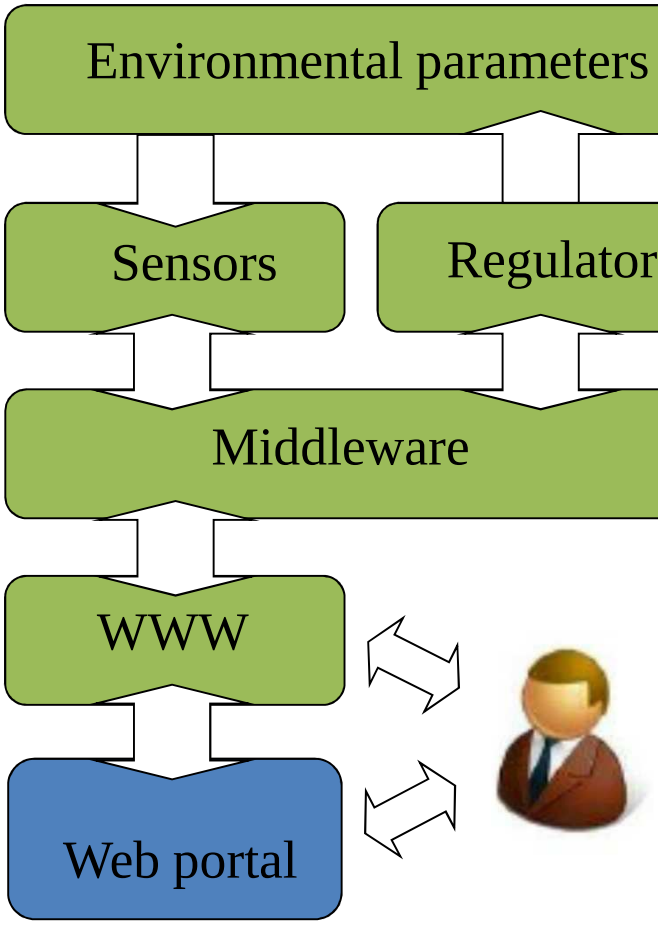
*WE LOOK AT ONE SUCH MODERN APPLICATION – THE SMART HOMES AND ITS NUMEROUS AUTOMATED DEVICES THAT ALLOW:*

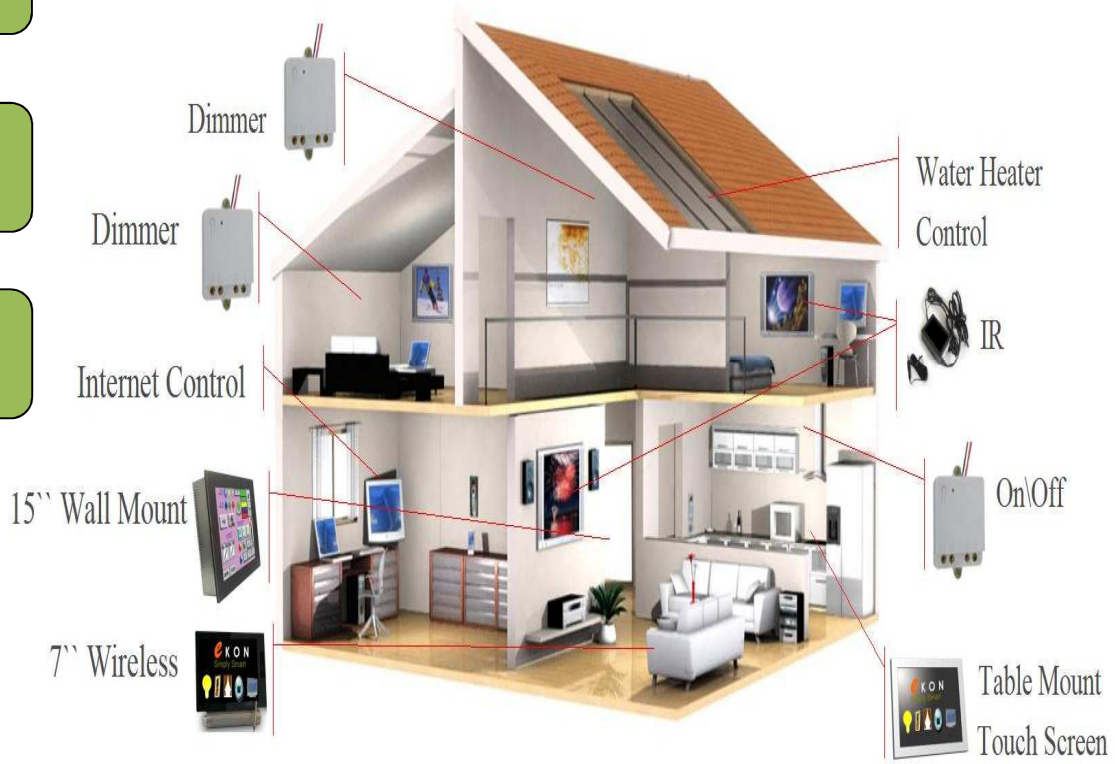
- REMOTE ACCESS TO AIR CONDITIONING, HOUSEHOLD MACHINES, HOUSE CLEANING AND LIGHT SYSTEM (INCLUDING ENERGY EFFICIENCY APPLICATIONS);

- SPECIFIC APPLICATIONS AS ELDERCARE AND CHILDCARE;

- VIRTUAL & AUGMENTED REALITIES IMPLEMENTATION.

# SMART HOME – MONITORING CONCEPT

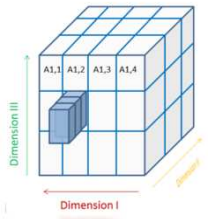


# Methodological approach to threats identification

- We assume that smart homes are cyber-physical systems encompassing both technologies and human factors;

- The main idea is to chose the factors in a system (we call them **dimensions**) with their varieties (we call them **alternatives**) and to run scenarios encompassing different alternatives from multiple dimensions

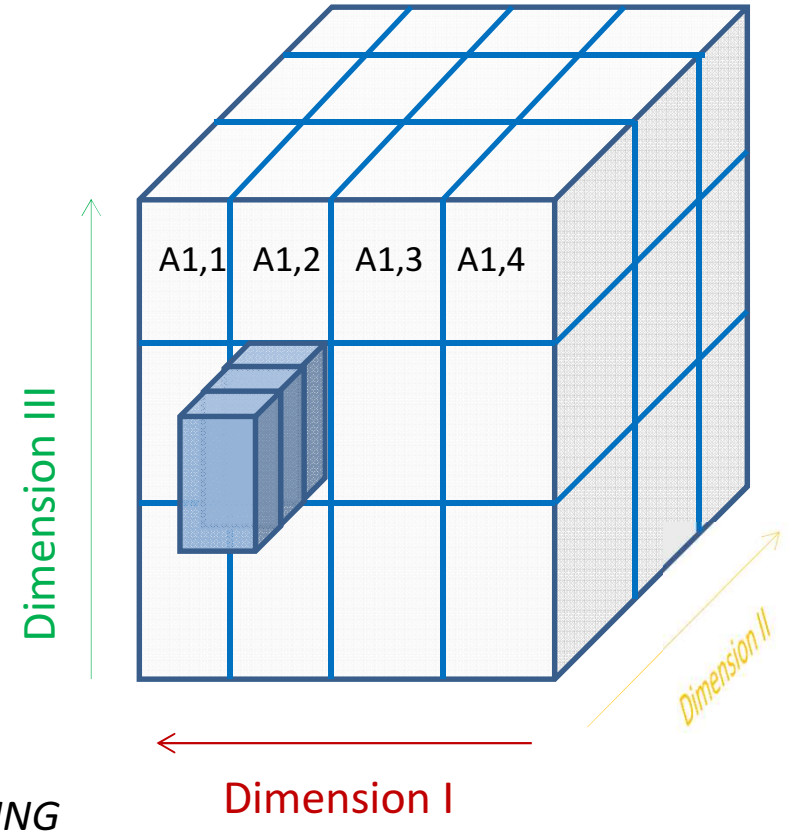


# Problem Space Definition

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 | | |

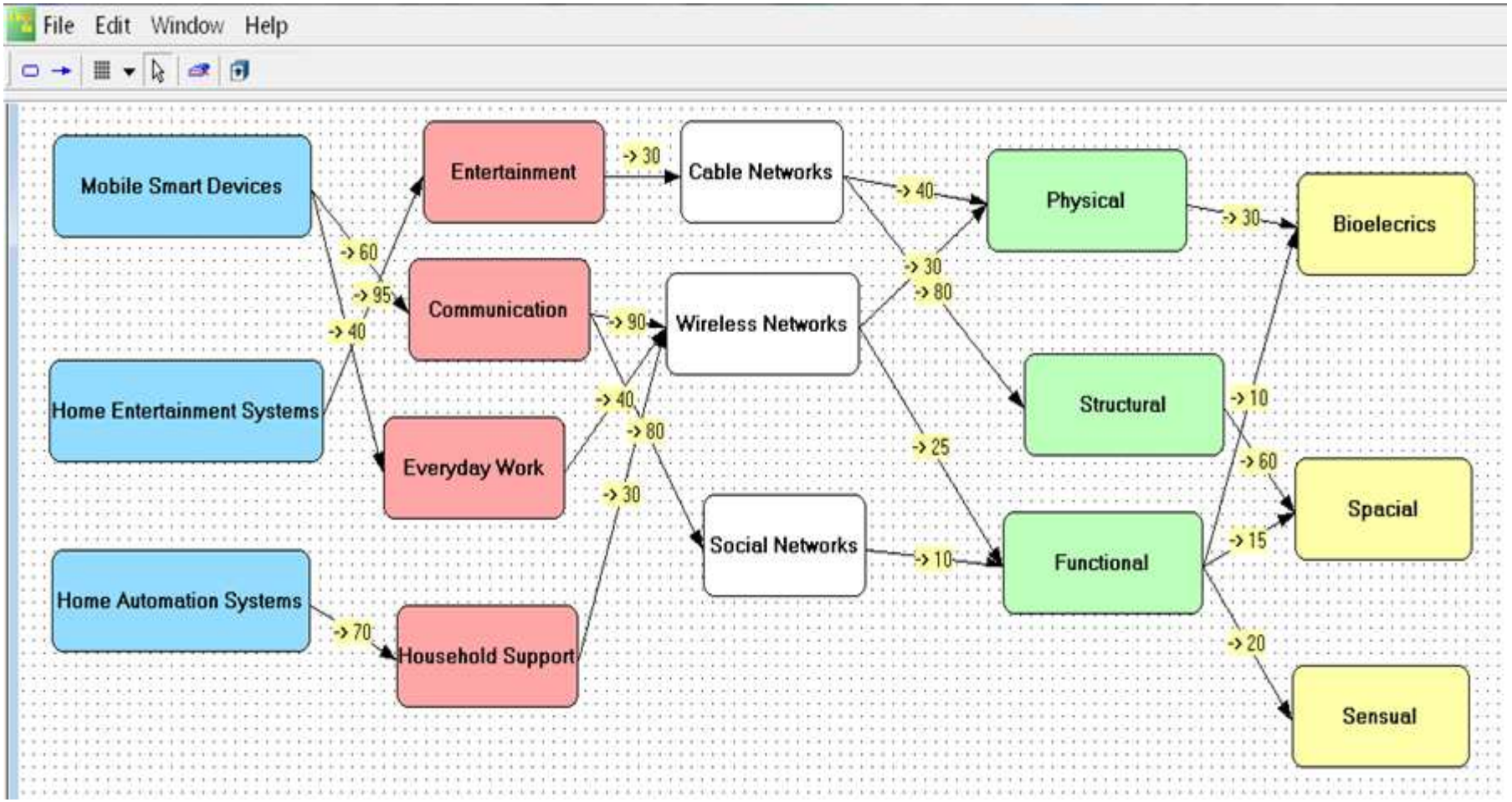
## Morphological Analysis




*Brainstorming & Q-based Delphi info gathering*

# Software Implementation with examples

## Maximum scenario combinations: 5x3x4x3x3x3 = 1620



I-SCIP-MA

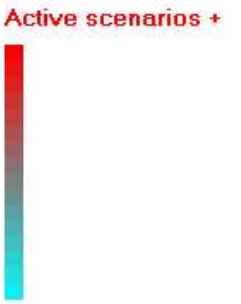
# RESULTING SCENARIOS

Selected Scenarios Set

Morphological Analysis

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

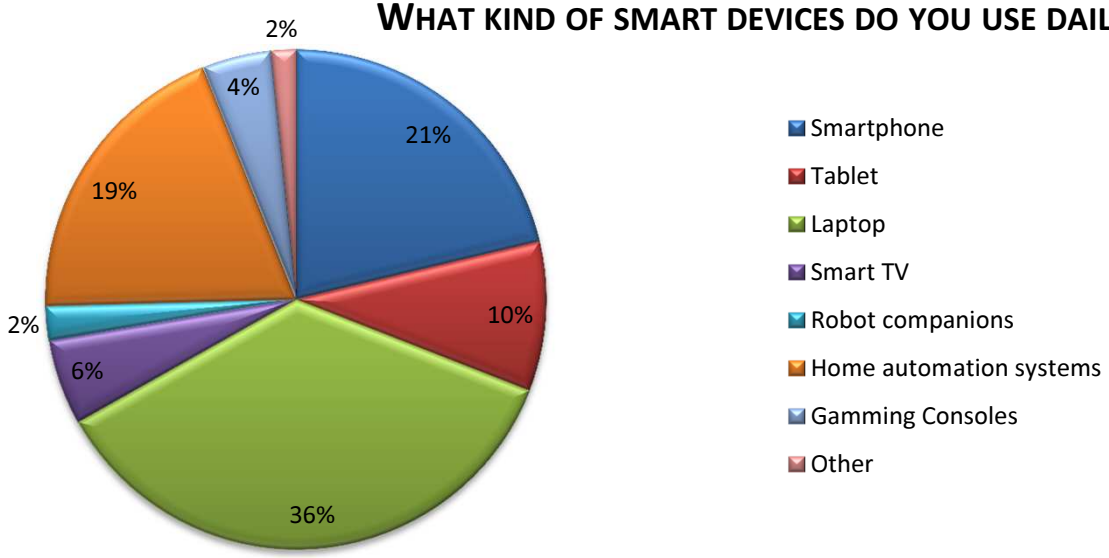
| Index | Length | Weight | Name |
|---|---|---|---|
| 1 | 5 | 170 | Scenario1 |
| 2 | 5 | 125 | Scenario2 |
| 3 | 5 | 265 | Scenario3 |
| 4 | 5 | 145 | Scenario3 |
| 5 | 5 | 195 | Scenario4 |
| 6 | 5 | 195 | Scenario5 |
| 7 | 5 | 140 | Scenario6 |
| 8 | 5 | 160 | Scenario7 |
| 9 | 5 | 210 | Scenario8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



# Ongoing work

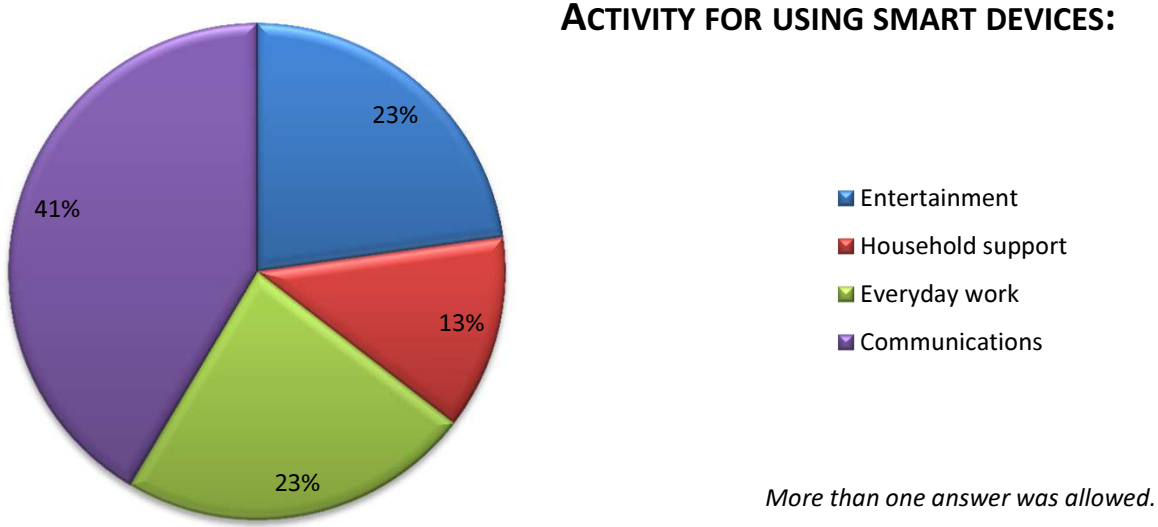
- We have carried out a survey with 152 participants – people in their early 20-ies;
- Agent based modeling is being carried out related to different scenario context;
- Environmental sensor system is being developed and deployed;
- On-hand experiments planned to start soon.

## WHAT KIND OF SMART DEVICES DO YOU USE DAILY?




*More than one answer was allowed.*

## ACTIVITY FOR USING SMART DEVICES:

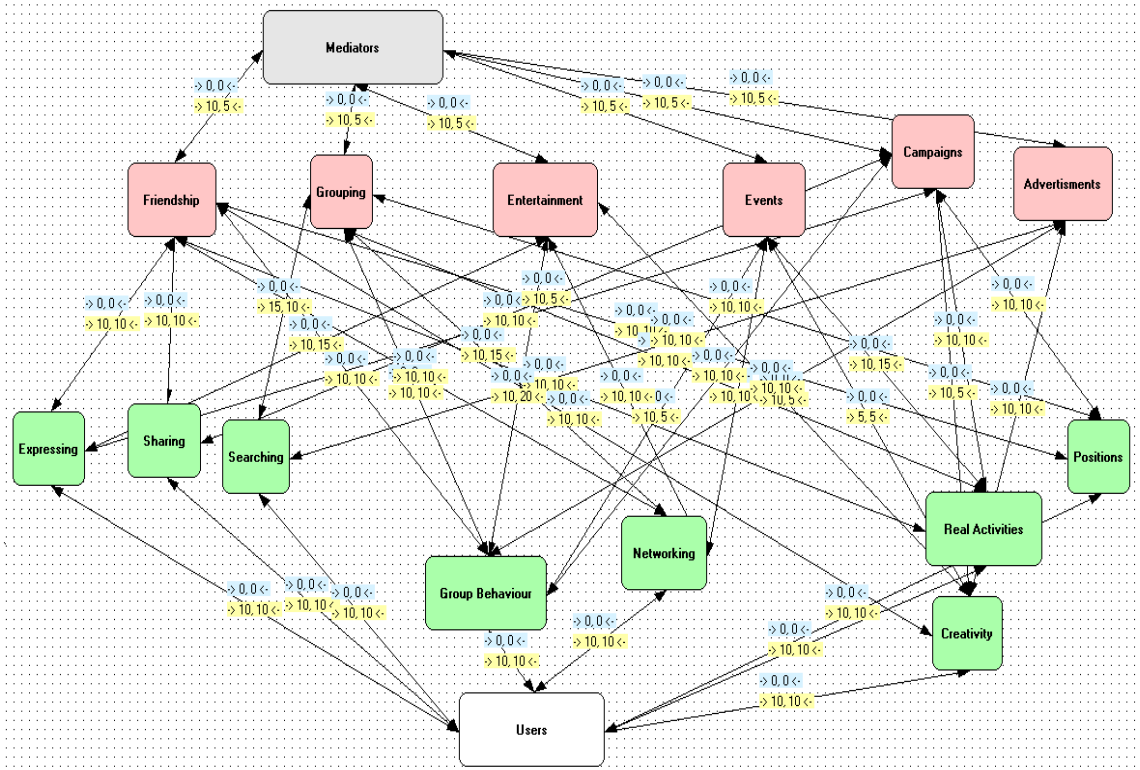


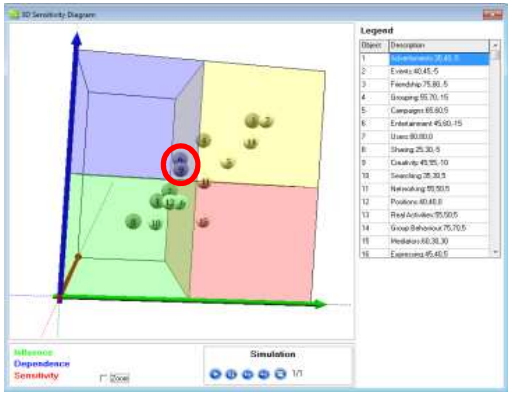

*More than one answer was allowed.*

# What's next?

I-SCIP-SA

## System Analysis for selected scenarios from the Morphological Analysis



*Social networks cyber threats identification example after [Minchev, 2012]*

# SUMMARY

*DEFINING OF A GENERAL CONTEXT FOR STUDYING SMART HOMES ENVIRONMENTS CYBER THREATS REQUIRES A COMPLEX MIXTURE OF EXPERTS' OPINIONS, COMBINED WITH LITERATURE DATA AND REAL SENSORS SYSTEMS AVAILABILITY FOR RICH ENVIRONMENT AND HUMAN FACTOR MONITORING.*

*THIS COMPLEX MIXTURE IS FURTHER PROCESSED VIA MORPHOLOGICAL AND SYSTEMS ANALYSIS FOR GENERAL AND CONCRETE CYBER THREATS SCENARIOS SELECTION BASED ON EXPERTS KNOWLEDGE AND SOFTWARE SUPPORT TOOLS.*

# Acknowledgement

This study is financially supported by DFNI-T01/4 'A Feasibility Study on Cyber Threats Identification and their Relationship with Users' Behavioural Dynamics in Future Smart Homes', National Science Fund, Ministry of Education, Youth and Science, 2012 – 2014, www.smarthomesbg.com. The authors also express special gratitude for the experts data support to EU Network of Excellence in Managing Threats and Vulnerabilities for the Future Internet – SysSec FP7 project, Grant Agreement No 257007, 2007 – 2013, www.syssec-project.eu.

# THANK YOU FOR THE ATTENTION!