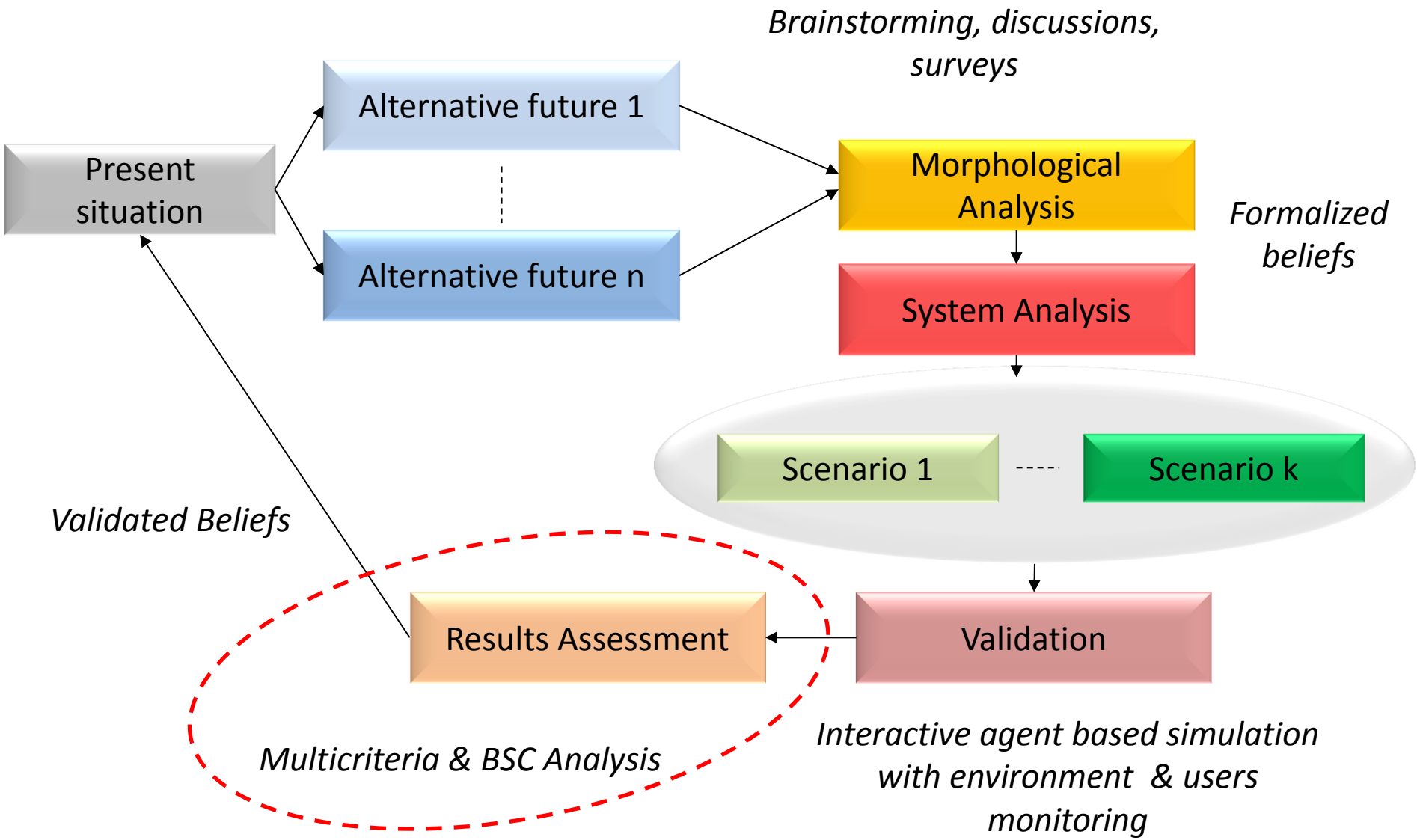
MULTICRITERIA ASSESSMENT SCALE OF FUTURE CYBERTHREATS IDENTIFICATION

Zlatogor Minchev & Emil Kelevedjiev

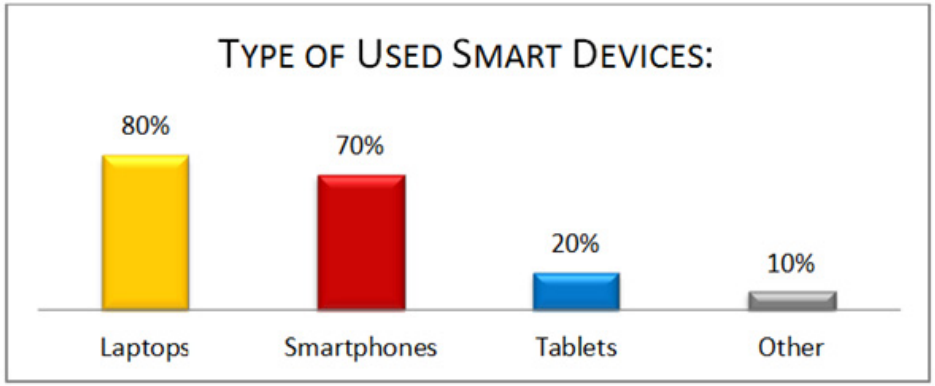
E-mails: zlatogor@bas.bg, keleved@math.bas.bg

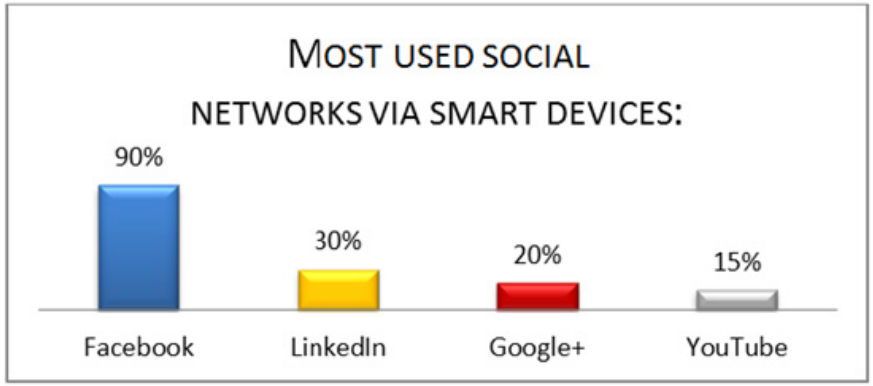
Sofia, Bulgaria Scientific Conference 'Mathematics Days in Sofia' July 9, 2014

METHODOLOGICAL FRAMEWORK



POTENTIAL SOURCES OF CYBERTHREATS GO SMART & FUTURE QUITE UNCERTAIN...





THREATS

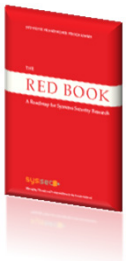
- Malware
- Targeted Attacks
- Social Engineering - Phishing

AREAS

- 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



...critical services; changing cybersecurity nature..
...we educate for the unknown...

Multicriteria Experts' Assessment Examples*

Social Networks Cyber Threats Multicriteria Assessment

Threat/Area	Human Factor	Digital Society	Governance	Economy	New Technologies	Environment of Living
Social Engineering						
Malware						
Spam & Scam						
Multimedia Influences						
Espionage & Privacy						

Smart Homes Cyber Threats Multicriteria Assessment

Threat/Area	Human Factor	Digital Society	Governance	Economy	New Technologies	Environment of Living
Targeted Attacks						
Compromised Devices						
Malware						
Technologies Influences						
Privacy & Allianation						

Risk levels for Web 2.0/Web3.0 Technological Progress Stage Assessments:

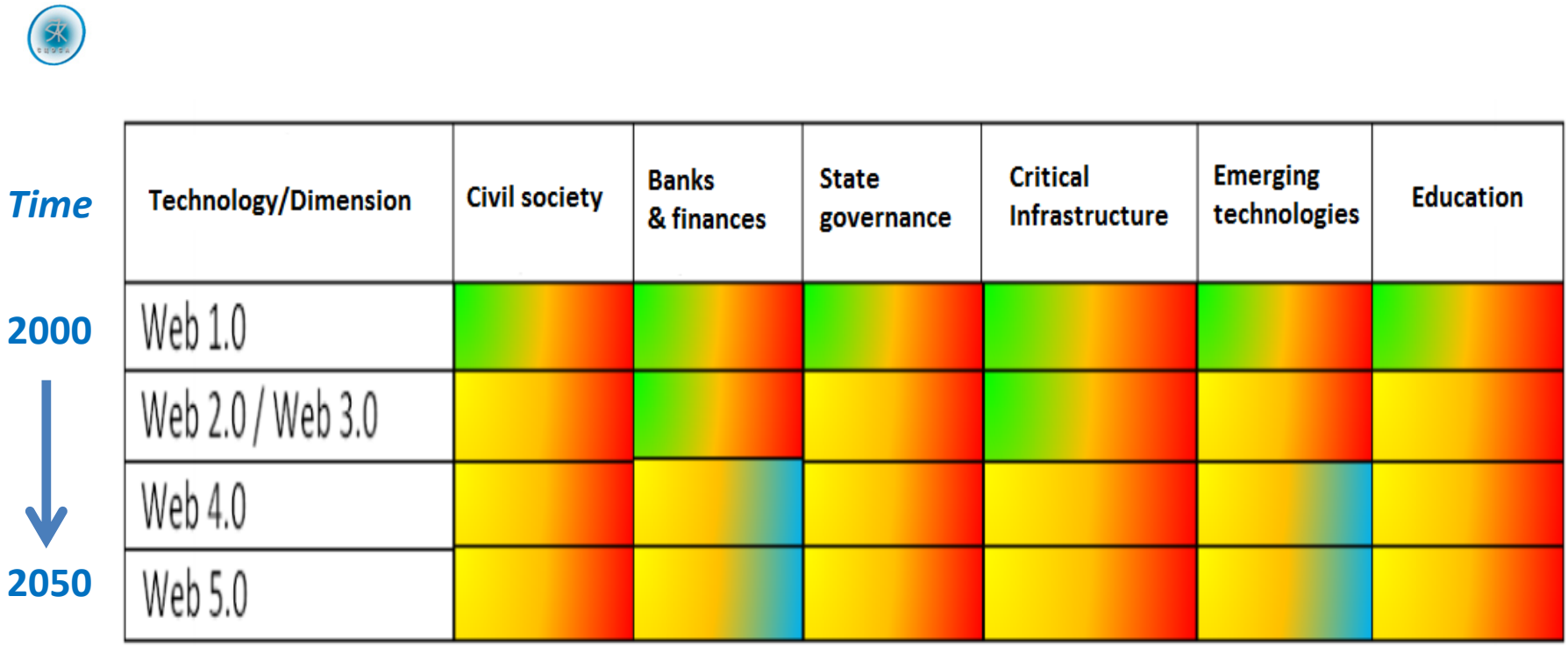
2, High

3, Severe

1, Uncertain

*The classification results are gathered from 75 national & international experts' brainstorming meeting discussions in the framework of DMU 03/22, DFNI T01/4 active collaboration with JTSAC in 2014.

Cyber Threats Multiple Risks Prognosis*



Risk levels:

- 5, Weak
- 4, Moderate
- 3, Severe
- 2, High
- 1, Uncertain

* The classification results are gathered from 250 national & international experts in the framework of Bulgarian Cyber security Strategy Draft preparation from JTSAC for Ministry of Defence in 2013.

Civil society

1) the aggregate of non-governmental organizations and institutions that manifest interests and will of citizens

2) individuals and organizations in a society which are independent of the government

Critical infrastructure

Most commonly associated with this term are facilities for:

- electricity (generation, transmission, etc);
- gas and oil production;
- telecommunication;
- water supply, food production and distribution;
- public health (hospitals, ambulances);
- transportation systems (railway network, airports), etc

An **Emerging technology** (as distinguished from a conventional technology) is a field of technology that broaches new territory in some significant way, with new technological developments.

Examples of currently emerging technologies include *educational technology, information technology, nanotechnology, biotechnology, cognitive science, robotics, and artificial intelligence.*

Model Description matrix a_{ij}
Reciprocal values of the estimates:

Time period	Threat 1	Threat 2	Threat 3	Threat 4	Threat 5	Threat 6
1	0.2	0.2	0.2	0.2	0.2	0.2
2	0.25	0.33	0.25	0.33	0.25	0.25
3	0.33	0.5	0.33	0.33	0.5	0.33
4	0.33	0.5	0.33	0.5	1	0.5

x_{ij} cost to prevent threat j at time period i

(e.g. billions of euros)

$y_i = \sum_j x_j$ cost in time period i

$y_1 < y_2 < y_3 <$ …

minimum of upper value ($u \approx 1$)

$x_{ij} > u$

Upper bound for
the total cost for all periods:

$$\sum_{i,j} x_{ij} < C$$

Objective function:
maximize the protection:

$$\sum_{i,j} a_{ij}\, x_{ij}$$

Linear Programming model,
but based on interaction
with users (experts)

LPSolve IDE v5.5.2.0

Authors

Henri Gourvest, William Pattton, Peter Notebaert

lp_solve

http://groups.yahoo.com/group/lp_solve

http://sourceforge.net/projects/lpsolve/files/lpsolve/

Michel Berkelaar	Kjell Eikland
Jeroen Dirks	Peter Notebaert

Third party components

SynEdit	http://synedit.sourceforge.net
VirtualTreeView	http://www.delphi-gems.com
XPMenu	http://www.shagrouni.com

We made some experiments
with sample data
(very artificially chosen)

Solution for costs x_{ij} based on u=1 and C=28

Time period	Threat 1	Threat 2	Threat 3	Threat 4	Threat 5	Threat 6
1	1	1.62	1	1.38	1	1
2	1	1	1	1	2	1
3	1.52	1	1	1.48	1	1
4	1.12	1	1.88	1	1	1

The same solution in terms of experts assessment

Time period	Civil Society	Banks & Finances	State Gover-nance	Critical Infra-structure	Emerging Technology	Education
2010	1	1.62	1	1.38	1	1
2020	1	1	1	1	2	1
2030	1.52	1	1	1.48	1	1
2040+	1.12	1	1.88	1	1	1

Discussion

Obviously, the identification of future cyber threats is a complex task, encompassing both: experts' knowledge and a suitable validation process. As 'validation in general' is difficult to be achieved, context dependent and goal oriented multicriteria optimization could be implemented. This in combination with experts' beliefs simulation produces a less uncertain, explanatory result, concerning the upcoming digital future cyber threats.

Acknowledgements

The authors express a special gratitude for the financial support to: A Study on IT Threats and Users' Behaviour Dynamics in Online Social Networks, DMU03/22, Bulgarian Science Fund, Young Scientists Grant, 2011-2014, WWW.SNFACTOR.COM

Explicit thanks for the smart environments cyber threats scenario context to: 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

A special gratitude for the general cyber landscape context to: EU Network of Excellence in Managing Threats & Vulnerabilities for the Future Internet, SYSSEC, EU FP 7, 2010-2014, WWW.SYSSEC-PROJECT.EU

THANK YOU FOR YOUR ATTENTION!